ΣΤΡΑΤΙΩΤΙΚΗ ΣΧΟΛΗ ΕΥΕΛΠΙΔΩΝ
Τμήμα Στρατιωτικών Επιστημών

ΠΟΛΥΤΕΧΝΕΙΟ ΚΡΗΤΗΣ
Σχολή Μηχανικών Παραγωγής

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΑΤΡΙΒΗ ΜΕ ΘΕΜΑ :

‘’ΚΡΥΠΤΑΝΑΛΥΣΗ ΜΕ ΧΡΗΣΗ ΜΕΘΟΔΩΝ ΤΕΧΝΗΤΗΣ ΝΟΗΜΟΣΥΝΗΣ’’

Μαρία Μπογιαννίδου
Α.Μ.: 2018018027

Περιεχόμενα

Keywords

Κρυπτανάλυση, Μέθοδοι Τεχνητής Νοημοσύνης, Εξελικτικός Υπολογισμός, Τεχνητά Νευρωνικά Δίκτυα, Particle Swarm Optimization, Differential Evolution, Διαφορική Κρυπτανάλυση, block ciphers, Feistel ciphers, Speck cipher

“All the magic crypto fairy dust in the world won’t make you secure.”— Gary McGraw

Think of it. A digital computer. Electrical brain.
Alan Turing

Those who can imagine anything, can create the impossible.
Alan Turing

Αφιερωμένη,
στους γονείς μου, που πάντα πίστευαν σε μένα και με έκαναν αυτό που είμαι σήμερα και στον σύντροφο μου, που με στηρίζει, με βοηθάει και με κατανοεί όλα αυτά τα χρόνια.

ΠΕΡΙΛΗΨΗ

Η παρούσα μεταπτυχιακή διατριβή αφορά στην κρυπτανάλυση με χρήση μεθόδων τεχνητής νοημοσύνης. Η κρυπτανάλυση, η αποκωδικοποίηση δηλαδή κρυπτογραφημένων πληροφοριών, αποτελεί πρόκληση ανά τους αιώνες. Εκτός από την εφαρμογή της για την απόκτηση πληροφοριών στις οποίες δεν επιτρέπεται η πρόσβαση, χρησιμοποιείται επίσης και για να εντοπίζει τις αδυναμίες και τα τρωτά σημεία κάθε κρυπτοσυστήματος, πριν αυτό εφαρμοστεί. Η κρυπτανάλυση είναι ένα πολύ σημαντικό βήμα στον έλεγχο της δύναμης κάθε κρυπτοσυστήματος.

Την τελευταία δεκαετία έχει παρατηρηθεί ένα αυξανόμενο ενδιαφέρον στην εφαρμογή μεθόδων Τεχνητής Νοημοσύνης σε προβλήματα που προκύπτουν στον τομέα της κρυπτογραφίας και της κρυπτανάλυσης. Αυτό συμβαίνει λόγω της αποτελεσματικότητας των μεθόδων αυτών στον χειρισμό δύσκολων προβλημάτων και στον ιδιαιτέρως σπουδαίο ρόλο των αυτοματοποιημένων τεχνικών στον σχεδιασμό και στην κρυπτανάλυση κρυπτοσυστημάτων. Η τεχνητή και υπολογιστική νοημοσύνη έχουν αρκετά κοινά χαρακτηριστικά με την επιστήμη της κρυπτολογίας, ιδιαίτερα με την κρυπτανάλυση. Κάποια από αυτά είναι η επεξεργασία μεγάλου όγκου δεδομένων και οι εργασίες σε μεγάλους χώρους αναζήτησης . Ο κρυπταναλυτής ψάχνει το κατάλληλο κλειδί για κάθε συγκεκριμένη αποκρυπτογράφηση μέσα σε πολλές πληροφορίες και η τεχνητή νοημοσύνη μια κατάλληλη λύση σε ένα πλήθος πιθανών λύσεων. Αυτή η εργασία λοιπόν, θα παρουσιάσει αλγόριθμους και μεθόδους τεχνητής νοημοσύνης που χρησιμοποιούνται για κρυπτανάλυση.

Αρχικά θα παρουσιαστούν βασικοί ορισμοί και έννοιες και θα γίνει μία μικρή ιστορική αναδρομή. Έπειτα, θα αναλυθούν οι Κρυπτογραφικοί Αλγόριθμοι Δέσμης (Block ciphers), με έμφαση στις συμμετρικές δομές Feistel και τον κρυπταλγόριθμο DES (Data Encryption Standard).Στην συνέχεια, θα αναλυθούν οι αλγόριθμοι που έχουν εμπνευστεί από την φυσική εξέλιξη και την κοινωνική συμπεριφορά, δηλαδή οι αλγόριθμοί Εξελικτικού Υπολογισμού (Evolutionary Computation-EC). Έμφαση θα δοθεί στον αλγόριθμο PSO (Particle Swarm Optimization, ’’Βελτιστοποίησης Σμήνους Σωματιδίων ‘’).

Τα επόμενα που θα παρουσιαστούν θα είναι τα Τεχνητά Νευρωνικά Δίκτυα (Artificial Neural Networks ,ANN) και οι διάφορες εφαρμογές τους, όπως στην κρυπτογραφία ελλειπτικών καμπυλών. Στη συνέχεια, θα αναλυθεί ένα είδος των ΑΝΝ, το Πολυωνυμικό Νευρικό Δίκτυο Κορυφογραμμής (Ridge Polynomial Network -RPN). Τέλος, θα επισημανθούν παρατηρήσεις μέσα από την παρουσίαση πινάκων αποτελεσμάτων πειραμάτων.

Στο κεφάλαιο 6 θα παρουσιαστεί μία μελέτη για την κρυπτανάλυση του κρυπτογραφήματος Speck32/64 με χρήση νευρωνικών distinguishers και δικτύων. Το Speck θεωρείται ένα από το πιο απροσπέλαστα κρυπτογραφήματα και η κρυπτανάλυση του αποτελεί μεγάλη πρόκληση. Κυρίως έχει επιτευχθεί σε Speck μειωμένων επαναλήψεων.

Κάποιες έννοιες δυστυχώς δεν υπάρχουν στην ελληνική ορολογία και θα αναγράφονται στα αγγλικά. Στο τέλος υπάρχει ένα κεφάλαιο με παρουσίαση της ορολογίας και ανάλυση διάφορων εννοιών που θα αναφερθούν στην παρούσα διατριβή και θεώρησα ότι χρήζουν επεξήγησης.

ΕΙΣΑΓΩΓΗ

1. Γενικές πληροφορίες Κρυπτολογίας.

Οι άνθρωποι πάντα είχαν πληροφορίες ή μυστικά ,άλλα περισσότερο σημαντικά και άλλα όχι ,που δεν ήθελαν να γίνουν γνωστά σε τρίτους. Στην αντίπερα όχθη, πάντα υπήρχε η ανάγκη να καταφέρει κάποιος να αποκτήσει αυτή την κρυμμένη, μυστική πληροφορία ενός άλλου. Όλη αυτή η διαδικασία και οι τρόποι απόκρυψης της πληροφορίας, αλλά και η αντίστροφη της, γέννησαν την επιστήμη της κρυπτολογίας.

Κρυπτολογία είναι ο κλάδος της επιστήμης ο οποίος ασχολείται με τη μελέτη και σχεδίαση κρυπτογραφικών τεχνικών, συστημάτων και πρωτοκόλλων (κρυπτογραφία), καθώς και με τη μελέτη διαδικασιών για την παραβίαση αυτών (κρυπτανάλυση). Συνεπώς, η κρυπτολογία από τη μία πλευρά ασχολείται με την απόκρυψη και από την άλλη με την αποκάλυψη του περιεχομένου ενός κωδικοποιημένου μηνύματος. Σήμερα η κρυπτολογία θεωρείται ένα διεπιστημονικό γνωστικό πεδίο, το οποίο μπορεί να μελετηθεί ως όψη των εφαρμοσμένων μαθηματικών, της θεωρητικής πληροφορικής ή της επιστήμης ηλεκτρονικού μηχανικού. Η σημασία της κρυπτολογίας είναι τεράστια στους τομείς της ασφάλειας υπολογιστικών συστημάτων και των τηλεπικοινωνιών.

Η ρίζα της κρυπτολογίας έγκειται στην προσπάθεια αποστολής μηνυμάτων το περιεχόμενο των οποίων θα προστατεύεται, ώστε να αναγνωστεί μόνο από τον επιθυμητό παραλήπτη. Αυτός ο πόθος οδήγησε στην επινόηση τεχνικών οι οποίες επιτρέπουν τον μετασχηματισμό των δεδομένων, με τέτοιο τρόπο ώστε να είναι αδύνατη η υποκλοπή του περιεχομένου τους κατά τη διαδικασία αποστολής ή αποθήκευσης. Η διαδικασία μετασχηματισμού των πληροφοριών ονομάζεται κρυπτογράφηση και η αντίστροφή της αποκρυπτογράφηση. Το σύνολο των βημάτων και των κανόνων οι οποίοι καθορίζουν την κρυπτογράφηση και την αποκρυπτογράφηση καλείται κρυπτογραφικός αλγόριθμος. Η σημερινή κρυπτογραφία εξετάζει κρυπτογραφικούς αλγορίθμους από τη σκοπιά των ηλεκτρονικών υπολογιστών και με σημαντική θεωρητική βάση στα μαθηματικά (π.χ. θεωρία αριθμών, θεωρία πληροφορίας κλπ.). Η κρυπτανάλυση εξετάζει τις μεθόδους μελέτης και αποκρυπτογράφησης ενός προστατευμένου μηνύματος, χωρίς όλη η απαραίτητη πληροφορία προς αυτόν τον σκοπό να είναι διαθέσιμη.

Η κρυπτανάλυση είναι η μελέτη για την επινόηση μεθόδων για να κατανοηθεί η κρυπτογραφημένη πληροφορία και έχει ως στόχο να βρει το κλειδί, το μήνυμα ή τον αλγόριθμο που με βάση αυτό, κρυπτογραφήθηκε το μήνυμα. Βασικός στόχος της είναι, ανάλογα με της απαιτήσεις του αναλυτή κρυπτοσυστημάτων ή αλλιώς κρυπταναλυτή , να βρει το κλειδί, το μήνυμα ή ένα ισοδύναμο αλγόριθμο που θα τον βοηθά να αναγνώσει το (κρυφό) μήνυμα. Ένας κρυπταλγόριθμος λέγεται ότι έχει «σπάσει», αν βρεθεί μια μέθοδος (πιθανοκρατική ή ντετερμινιστική) που μπορεί να βρει το μήνυμα ή το κλειδί με πολυπλοκότητα μικρότερη από την πολυπλοκότητα της επίθεσης ωμής βίας (αγγλ.: brute force attack). Η πρώτη νύξη σχετικά με την κρυπτανάλυση έγινε από ένα Άραβα μαθηματικό τον 8ο αιώνα με την εργασία Ανταμπ-αλ-κουταπ ή αλλιώς Εγχειρίδιο των γραμματέων.

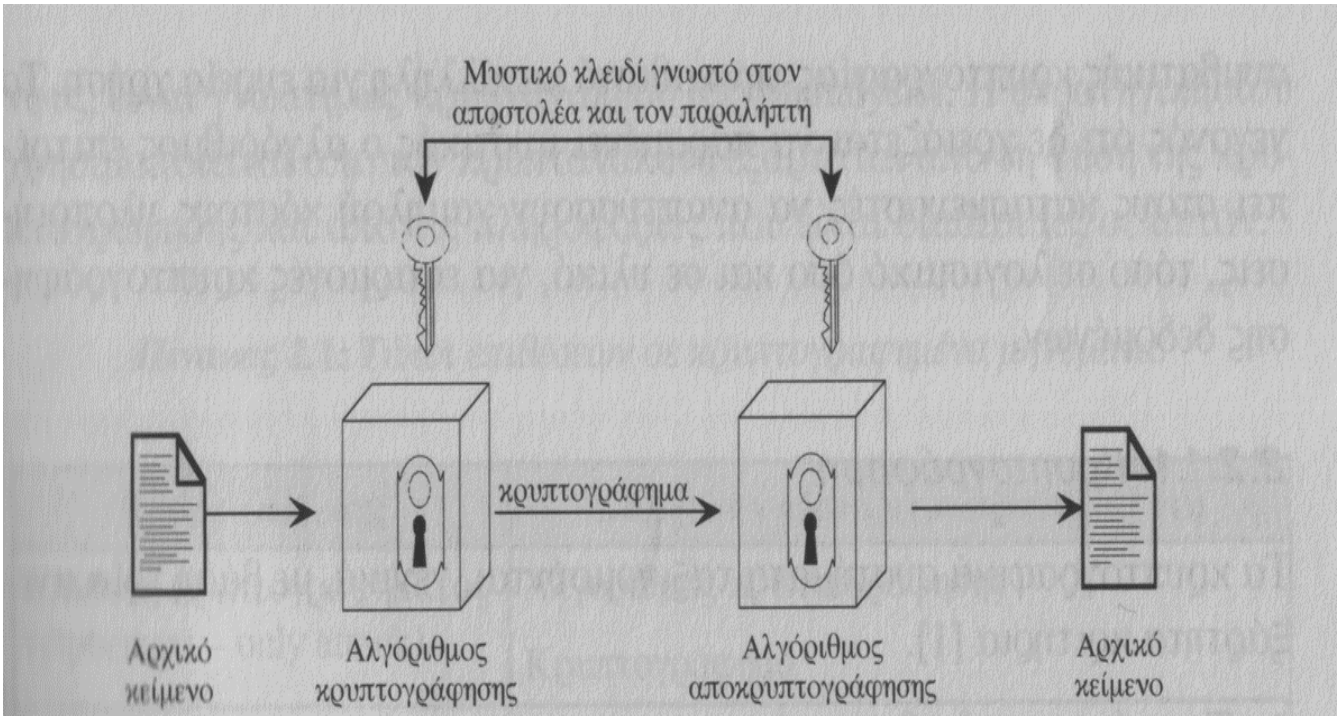
Η κρυπτανάλυση όμως δεν έχει μόνο ως άμεσο σκοπό την υποκλοπή. Η κρυπτανάλυση ταυτοποιεί τις αδυναμίες των κρυπτογραφημάτων και ερευνά μεθόδους για να τις εκμεταλλευτεί έτσι ώστε να συνθέσει το κλειδί ή/και το κείμενο που κρυπτογραφήθηκε. Από τους τρόπους με τους οποίους μπορεί ένας αλγόριθμος να ¨σπάσει¨, οδηγούμαστε σε ασφαλέστερες δομές και τεχνικές με αποτέλεσμα να κατασκευαστούν πιο ασφαλείς αλγόριθμοι.

Σήμερα η κρυπτολογία θεωρείται ένα διεπιστημονικό γνωστικό πεδίο, το οποίο μπορεί να μελετηθεί ως όψη των εφαρμοσμένων μαθηματικών, της θεωρητικής πληροφορικής ή της επιστήμης ηλεκτρονικού μηχανικού. Παρεμφερείς κλάδοι είναι, αντιστοίχως, η στεγανογραφία και η στεγανοανάλυση.

Η κρυπτολογία είναι μια επιστήμη που επηρέασε σημαντικά την παγκόσμια ιστορία. Αποτελεί ένα κρίσιμο τομέα και στο πεδίο των στρατιωτικών επιχειρήσεων φυσικά. Οι ένοπλες δυνάμεις κάθε χώρας οφείλουν να προστατεύουν την εθνική ασφάλεια, διαφυλάσσοντας τις πληροφορίες και τα σχέδια επιχειρήσεων που τις αφορούν .Και στον τομέα των επιχειρήσεων όμως, παίζει σημαντικό ρόλο ,καθώς όσο αυξάνεται ο ανταγωνισμός των επιχειρήσεων στο σύγχρονο ανταγωνιστικό περιβάλλον, τόσο ανθεί η βιομηχανική κατασκοπεία.

2. Κλασσικά Μοντέλα Κρυπτογράφησης - Αποκρυπτογράφησης

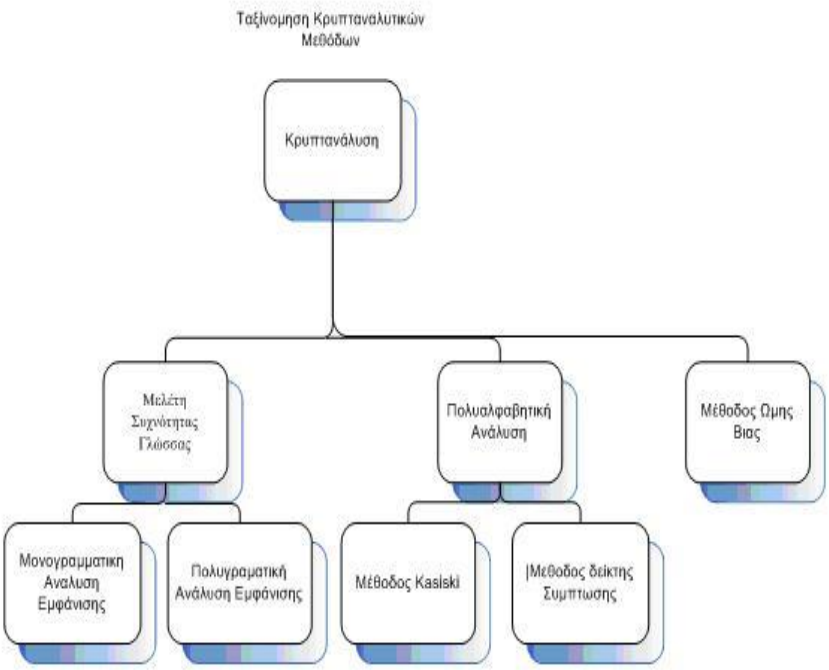
ΚΛΑΣΣΙΚΟ ΜΟΝΤΕΛΟ ΚΡΥΠΤΟΓΡΑΦΗΣΗΣ



Το αρχικό κείμενο κωδικοποιείται με τον αλγόριθμο κρυπτογράφησης (cipher) και το κλειδί (key) και μετατρέπεται σε κρυπτογράφημα. Η εμπιστευτικότητα βασίζεται κυρίως στο κλειδί κρυπτογράφησης. Με τον αλγόριθμο αποκρυπτογράφησης, ο παραλήπτης καταφέρνει να έχει το αρχικό κείμενο. Το μέγεθος του κλειδιού κρυπτογράφησης μετριέται σε αριθμό bits. Όσο μεγαλύτερο είναι το κλειδί κρυπτογράφησης, τόσο δυσκολότερα μπορεί να αποκρυπτογραφηθεί το κρυπτογραφημένο μήνυμα από επίδοξους εισβολείς. Διαφορετικοί αλγόριθμοι κρυπτογράφησης απαιτούν διαφορετικά μήκη κλειδιών για να πετύχουν το ίδιο επίπεδο ανθεκτικότητας κρυπτογράφησης.

3. Κρυπτανάλυση Κλασσικών Κρυπτοσυστημάτων

Υπάρχουν διάφοροι τύποι κρυπταναλυτικών επιθέσεων για τα κλασικά κρυπτοσυστήματα. Οι περισσότερες βασίστηκαν πάνω στην γλωσσική δομή του μηνύματος. Στις νεότερες μορφές Κρυπτανάλυσης Κλασικών Κρυπτοσυστημάτων παρατηρείται η είσοδος της στατιστικής στην ανάλυση.



4. Κρυπτανάλυση Σύγχρονων Κρυπτοσυστημάτων

Οι μέθοδοι για την κρυπτανάλυση σύγχρονων κρυπτοσυστημάτων είναι οι εξής:

- Διαφορική Κρυπτανάλυση (Differential Cryptanalysis)
- Γραμμική Κρυπτανάλυση (Linear Cryptanalysis)
- Κρυπτανάλυση στο Επίπεδο Υλικού (Side-channel cryptanalysis)
- Κλειδοσχεσιακή Κρυπτανάλυση (Releted Key Cryptanalysis)
- Κρυπτανάλυση Ισοτίμων (Cryptanalysis mod n)
- Κρυπτανάλυση τετραγώνου (Square Cryptanalysis)
- Στατιστική κρυπτανάλυση (Statistical Cryptanalysis)

5. Ταξινόμηση Μοντέλων Ασφαλείας

Υπάρχουν 4 βασικά μοντέλα για την αξιολόγηση των αλγορίθμων, τους οποίους καλούμαστε να κρυπταναλύσουμε :

α. Ασφάλεια άνευ όρων (Τέλεια Ασφάλεια)

Αυτή η μέτρηση εστιάζεται στην διάκριση αν ένα κρυπτοσύστημα έχει ασφάλεια άνευ όρων. Η βασική υπόθεση είναι ότι όσο κρυπτοκείμενο και αν κατέχει ο αντίπαλος, δεν υπάρχει αρκετή πληροφορία για να ανακτήσει το ανοικτό κείμενο (μοναδική λύση), όση υπολογιστική ισχύ (άπειρη) και αν έχει στην διάθεση του. Χαρακτηριστικό παράδειγμα το σημειωματάριο μίας χρήσης.

β. Υπολογιστική ασφάλεια (Πρακτική Ασφάλεια)

Αυτή η μέτρηση εστιάζεται στην υπολογιστική προσπάθεια "παράγοντας εργασίας", που χρειάζεται για να διασπαστεί ένα κρυπτοσύστημα. Στόχος των συγχρόνων συστημάτων είναι να εμφανίζουν μεγάλο παράγοντα δυσκολίας ώστε να μην είναι χρονικά δυνατό να διασπαστούν με τα διαθέσιμα (ή και τα μελλοντικά) μέσα.

γ. Ασφάλεια – θεωρία πολυπλοκότητας

Αυτή η μέτρηση εστιάζει στην ταξινόμηση της υπολογιστικής ικανότητας του αντιπάλου υπολογιστικών προβλημάτων ανάλογα με τους πόρους που απαιτούνται για την επίλυση τους. Οι πόροι αναφέρονται σε:

- Το μέγεθος δεδομένων που χρειάζονται σαν είσοδος στην επίθεση
- Τον υπολογιστικό χρόνο που χρειάζεται για να εκτελεστεί η επίθεση
- Το μέγεθος του χώρου αποθήκευσης που χρειάζεται για την επίθεση
- Το πλήθος των επεξεργαστών
- Αποδείξιμη ασφάλεια

δ. Αποδείξιμη Ασφάλεια

Αυτή η μέτρηση εστιάζεται στην απόδειξη ισοδυναμίας του μαθηματικού μοντέλου του κρυπτοσυστήματος με κάποιο πολύ γνωστό δύσκολο στην επίλυση του πρόβλημα (θεωρίας αριθμών). Χαρακτηριστικό παράδειγμα η παραγοντοποίηση μεγάλων ακεραίων.

6. Είδη Επιθέσεων

Η επίθεση για την κρυπτανάλυση μπορεί να γίνει είτε στον αλγόριθμο ή στο κανάλι επικοινωνίας.

6.1 Κρυπταναλυτικές επιθέσεις σε αλγορίθμους

Υπάρχουν έξι βασικές κρυπταναλυτικές επιθέσεις, κατηγοριοποιημένες ανάλογα με την ικανότητα του αντιπάλου (πόρους-υπολογιστική ισχύ) και το επίπεδο πρόσβασης που έχει ο επιτιθέμενος:

- Επιθέσεις εξαντλητικής αναζήτησης (Brute force attacks): Σε αυτές τις περιπτώσεις, ο επιτιθέμενος μπορεί να δοκιμάσει όλα τα δυνατά κλειδιά αποκρυπτογράφησης μέχρι να βρει το κλειδί που έχει χρησιμοποιηθεί.

- Επίθεση βασισμένη στο κρυπτοκείμενο (Ciphertext Only Attack-CO):Ο κρυπταναλυτής έχει στην διάθεση του N κρυπτομηνύματα με δεδομένη τη γνώση του αλγορίθμου. Σκοπός είναι να ανακαλύψει τα μηνύματα που περικλείουν τα κρυπτοκείμενα ή να εξαγάγει το κλειδί που χρησιμοποιήθηκε.

- Επίθεση βασισμένη στην γνώση μηνυμάτων κρυπτοκειμένων : Ο κρυπταναλυτής έχει στην διάθεση του μερικά ζευγάρια (μηνυμάτων, κρυπτοκειμένων). Ο στόχος είναι η εξαγωγή του κλειδιού ή ενός αλγορίθμου για την αποκρυπτογράφηση νέων μηνυμάτων (προσεγγιστικός αλγόριθμος) με το ίδιο κλειδί.

- Επίθεση βασισμένη στην επιλογή μηνυμάτων (Known Plaintext Attack KPA): Ο κρυπταναλυτής έχει καταφέρει να αποκτήσει πρόσβαση στη επιλογή του μηνύματος που θα κρυπτογραφηθεί. Στόχος είναι η εξαγωγή του κλειδιού ή ενός προσεγγιστικού αλγορίθμου.

- Προσαρμοσμένη επίθεση, βασισμένη στην επιλογή μηνυμάτων(Chosen Plaintex Attack CPA) : Ο κρυπταναλυτής μπορεί να επιλέξει όχι μόνο μία συστάδα μηνυμάτων αλλά μπορεί να επιλέξει ποιο επόμενο μήνυμα θα κρυπτογραφηθεί(Κατάλληλη επιλογή ζευγαριών προσδίδει περισσότερη πιθανότητα για την τιμή του κλειδιού). Στόχος είναι η εξαγωγή του κλειδιού ή ενός προσεγγιστικού αλγορίθμου.

- Επίθεση βασισμένη στην επιλογή κρυπτοκειμένων (Chosen Ciphertext Attack CCA): Ο κρυπταναλυτής μπορεί να επιλέξει κρυπτοκείμενα για αποκρυπτογράφηση (μελετά πώς συμπεριφέρεται ο αλγόριθμος στην αποκρυπτογράφηση) και έχει πρόσβαση στα αποκρυπτογραφημένα κείμενα.

- Προσαρμοσμένη επίθεση βασισμένη στην επιλογή μηνυμάτων - κλειδιών: Ο κρυπταναλυτής επιλέγει μια σχέση μεταξύ του άγνωστου κλειδιού και του δικό του κλειδιού και βάση των συμπερασμάτων που βγάζει από την ανάλυση (Είσοδος/έξοδος) στο σύστημα - στόχο και στο δικό του αντίγραφο (Κρυπταλγόριθμος) προσεγγίζει, μετά από κάποιες δοκιμές, το σωστό κλειδί.

6.2 Επιθέσεις στο κανάλι επικοινωνίας

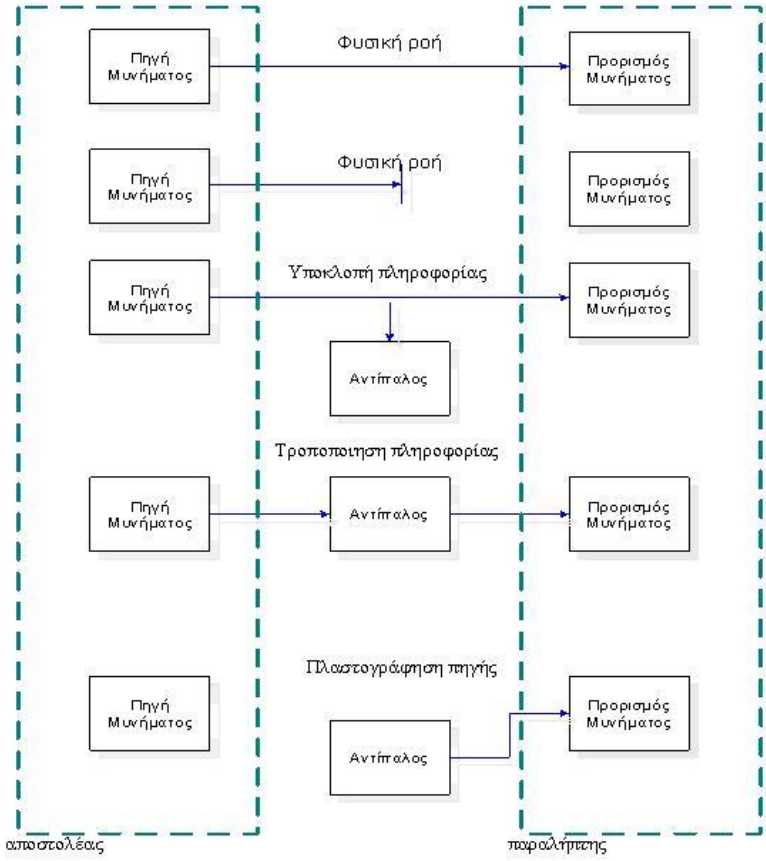
Υπάρχουν τέσσερεις βασικές απειλές στο κανάλι επικοινωνίας, κατηγοριοποιημένες με κριτήριο την ενεργή ή παθητική συμπεριφορά του αντιπάλου.

- Διακοπή γραμμής : Ο αντίπαλος έχει διακόψει την ροή της πληροφορίας από τον αποστολέα στον παραλήπτη (ενεργή συμπεριφορά).

- Υποκλοπή πληροφορίας από το κανάλι: Ο αντίπαλος αντιγράφει τις πληροφορίες που διαβιβάζονται στο κανάλι επικοινωνίας (παθητική συμπεριφορά – μη ανιχνεύσιμη).

- Τροποποίηση πληροφορίας στο κανάλι(Man-in-the-middle επίθεση): Ο αντίπαλος τροποποιεί τις πληροφορίες που διαβιβάζονται στο κανάλι με τέτοιο τρόπο, ώστε να αλλάξει το περιεχόμενο ή να αναγεννά δική του πληροφορία. (ενεργή συμπεριφορά).

- Πλαστογράφηση πηγής: Ο αντίπαλος προσποιείται ότι είναι ένα από τα μέλη που έχουν πρόσβαση στο κανάλι.

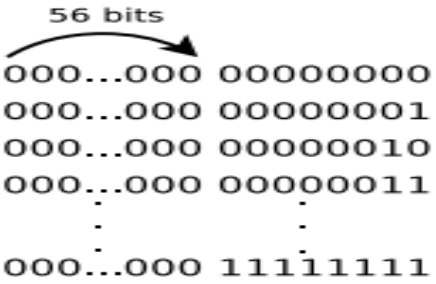


Στην παρούσα εργασία , θα αναλυθεί η διαδικασία με την οποία μπορεί κάποιος να ανακτήσει το κλειδί κρυπτογράφησης και να αποκρυπτογραφήσει πληροφορίες, με την βοήθεια μεθόδων τεχνητής νοημοσύνης.

7. Τεχνικές Επιθέσεων

Οι πιο γνωστές τεχνικές κρυπτανάλυσης είναι οι εξής :

- Ολοκληρωτική κρυπτανάλυση (Integral cryptanalysis) :Στην ολοκληρωτική κρυπτανάλυση αλγορίθμων, μελετώνται οι διαφοροποιήσεις οι οποίες παρουσιάζονται στο κρυπτογραφημένο κείμενο, όταν διαλέξουμε ένα σύνολο από αρχικά κείμενα για τα οποία κάποια συγκεκριμένα bits είναι κοινά σε όλα τους. Θα μπορούσαμε να πάρουμε το σύνολο των λέξεων των 64 bits για τις οποίες, τα πρώτα 56 bits είναι όλα μηδενικά και διαφέρουν μόνο στα 8 τελευταία bits. Επειδή η μέθοδος προσπαθεί να ΄αθροίσει΄΄ όλες τις επιμέρους διαφορές των αρχικών κειμένων, εμπνευσμένοι από την ανάλυση, δόθηκε το όνομα της Ολοκληρωτικής κρυπτανάλυσης. Μάλιστα, επειδή αρχικά σχεδιάστηκε για την κρυπτανάλυση ενός αλγορίθμου, του Square, πολύ συχνά στη βιβλιογραφία συναντάται με το όνομα του αλγορίθμου, Square cryptanalysis.



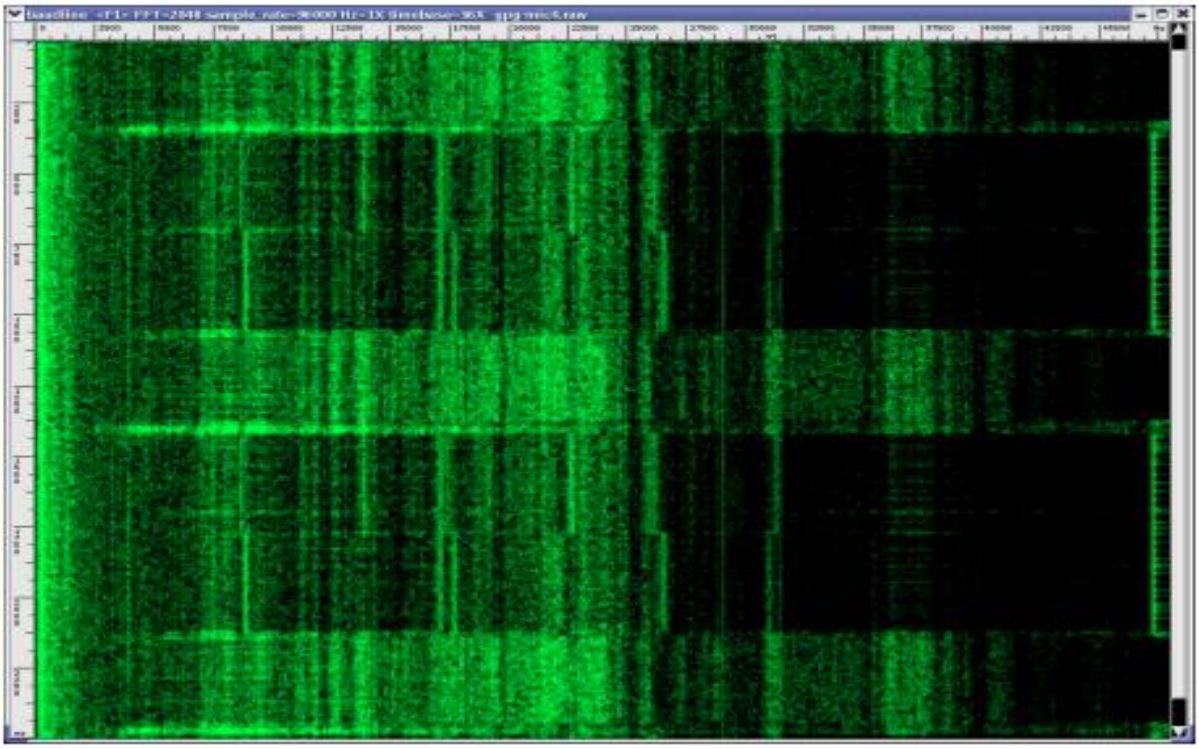
- Κρυπτανάλυση modulo N :Σε αυτό το είδος κρυπτανάλυσης, ο επιτιθέμενος προσπαθεί να δει αν και κατά πόσο ο αλγόριθμος παρουσιάζει κάποιες αποκλίσεις, όταν χρησιμοποιείται σε άλλο αριθμητικό σύστημα. Σαν επίθεση εισάγεται το 1999 από τους John Kelsey, Bruce Schneier και David Wagner προκειμένου να μελετηθεί η ασφάλεια κάποιων συγκεκριμένων αλγορίθμων.

- Κρυπτανάλυση κατατμήσεων (Partitioning cryptanalysis) : Οι Carlo Harpes, Gerard G. Kramer και James L. Massey , προσπαθώντας να γενικεύσουν τη γραμμική κρυπτανάλυση, οδηγήθηκαν στην κρυπτανάλυση κατατμήσεων. Η βασική ιδέα της επίθεσης, βασίζεται στην εύρεση μίας συνάρτησης Boole, η οποία να συνδυάζει τα bits του κλειδιού με τα bits του αρχικού κειμένου και τα bits του κρυπτογραφημένου κειμένου. Μία βασική διαφοροποίηση σε σχέση με τη γραμμική κρυπτανάλυση είναι η χρήση αρχικών και κρυπτογραφημένων κειμένων με ορισμένες αλγεβρικές και στατιστικές ιδιότητες.

- Επιθέσεις ολίσθησης (slide attacks) :Σε αυτή την κατηγορία επιθέσεων, η προσπάθεια επικεντρώνεται στον αλγόριθμο παραγωγής υποκλειδιών. Αν παρατηρηθεί κάποιο πρόβλημα στην κατασκευή τους από το αρχικό, τότε ενδέχεται αυτό το γεγονός να μπορεί να χρησιμοποιηθεί προκειμένου να αναπτυχθεί μία επίθεση σε ολόκληρο τον αλγόριθμο. Ένα πολύ κοινό τέτοιο πρόβλημα είναι η επανάληψη προηγούμενων υποκλειδιών, η άμεση αποκάλυψη μέρους του αρχικού κλειδιού κ.ά.

- Χρονικές επιθέσεις (Timing attacks) :Στις χρονικές επιθέσεις, ο επιτιθέμενος προσπαθεί να προσεγγίσει το κλειδί κάνοντας μετρήσεις στο χρόνο στον οποίο ο αλγόριθμος επιστρέφει τα αποτελέσματα. Για παράδειγμα στον RSA έχουμε πολλούς πολλαπλασιασμούς, όμως αν υπάρχουν πολλά μηδενικά το αποτέλεσμα υπολογίζεται γρηγορότερα σε σχέση με το να υπάρχουν περισσότερες μονάδες. Από αυτό το απλό γεγονός, ο επιτιθέμενος αν γνωρίζει ένα πλήθος αρχικών κειμένων μπορεί σε πολύ μεγάλο βαθμό να προσεγγίσει ένα κλειδί.

- Ακουστική κρυπτανάλυση (Timing attacks) :Μία παρόμοια προσέγγιση με τις χρονικές επιθέσεις, είναι αυτή των Adi Shamir και Eran Tromer. Σε αυτή τη προσέγγιση, ο επιτιθέμενος ηχογραφεί τον επεξεργαστή ο οποίος κρυπτογραφεί ένα μήνυμα. Από το ακουστικό κύμα ενδέχεται να μπορεί κανείς να ανακαλύψει την τιμή ορισμένων bits.



Ακουστικό κύμα ενός επεξεργαστή ο οποίος υπογράφει
ένα μήνυμα με τον αλγόριθμο RSA.

ΚΕΦΑΛΑΙΟ 1ο : Η ΙΣΤΟΡΙΑ ΤΗΣ ΚΡΥΠΤΑΝΑΛΥΣΗΣ

Η κρυπτανάλυση είναι άρρηκτα συνδεδεμένη με την κρυπτογραφία και η μία επιστήμη προωθεί και εξελίσσει την άλλη. Η κρυπτανάλυση εξελίσσεται για να μπορεί να αποκωδικοποιεί νέες μεθόδους κρυπτογραφίας και η κρυπτογραφία πρέπει συνεχώς να ανανεώνεται για να μπορεί να αντιμετωπίσει τις όλο και αποδοτικότερες επιθέσεις της πρώτης. Σε αυτό το κεφάλαιο θα γίνει μία ιστορική αναδρομή της πορείας και των δύο επιστημών.

1.1 Κλασσική περίοδος 1900 π.Χ.-1900 μ.Χ

Κατά την διάρκεια της αρχαιότητας η κρυπτογραφία ήταν αρκετά απλή και βασιζόταν στην ευρηματικότητα του κάθε δημιουργού , συνήθως γινόταν με αντικαταστάσεις γραμμάτων. Δεν χρειάζονταν εξειδικευμένες γνώσεις και πολύπλοκες συσκευές ούτε και για την κρυπτανάλυση συνεπώς.

Μία μικρή σφηνοειδής επιγραφή ανακαλύφθηκε στις όχθες του ποταμού Τίγρη και καταδεικνύει ότι οι πολιτισμοί που αναπτύχθηκαν στη Μεσοποταμία ασχολήθηκαν με την κρυπτογραφία ήδη από το 1500 π.Χ. Η επιγραφή αυτή περιγράφει μία μέθοδο κατασκευής σμάλτων για αγγειοπλαστική και θεωρείται ως το αρχαιότερο κρυπτογραφημένο κείμενο σύμφωνα με τον αρχαιολόγο Kahn.

Το αρχαιότερο βιβλίο κρυπτοκωδικών στον κόσμο, θεωρείται μία σφηνοειδής επιγραφή στα Σούσα της Περσίας. η οποία περιλαμβάνει τους αριθμούς 1 έως 8 και από το 32 έως το 35, τοποθετημένους τον ένα κάτω από τον άλλο, ενώ απέναντι τους βρίσκονται τα αντίστοιχα για τον καθένα σφηνοειδή σύμβολα.

Παρακάτω θα παρουσιαστούν κάποιες γνωστές μέθοδοι κρυπτογράφηση της αρχαιότητας και ο τρόπος που έγινε η κρυπτανάλυση τους.

1.1.1 Μέθοδος Μετάθεσης

Η πρώτη στρατιωτική χρήση της κρυπτογραφίας αποδίδεται στους Σπαρτιάτες. Τον 5ο αιώνα εφηύραν την σκυτάλη, την πρώτη κρυπτογραφική συσκευή, στην οποία το μήνυμα κρυπτογραφούνταν με την μέθοδο της μετάθεσης.

Η «Σπαρτιατική Σκυτάλη», όπως αναφέρει και ο Πλούταρχος, ήταν μια ξύλινη ράβδος, ορισμένης διαμέτρου, γύρω από την οποία ήταν τυλιγμένη ελικοειδώς μια λωρίδα περγαμηνής. Το κείμενο ήταν γραμμένο σε στήλες, ένα γράμμα σε κάθε έλικα και γραφόταν ενώ ήταν τυλιγμένο στην σκυτάλη. Κατόπιν αφαιρούνταν από την σκυτάλη. Όταν κάποιος ξετύλιγε τη λωρίδα, το κείμενο ήταν ακατάληπτο εξαιτίας της αναδιάταξης των γραμμάτων.

ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ:

Το «κλειδί» ήταν η διάμετρος της σκυτάλης. Η αποκρυπτογράφηση δηλαδή γινόταν αν η περγαμηνή τυλιγόταν σε μία σκυτάλη ίσης διαμέτρου.

1.1.2 Ιερογλυφικά-Γραμμική Α'&Β'

Τον 3ο και 2ο αιώνα π.Χ. εμφανίζεται η Κρητική εικονογραφική ή ιερογλυφική γραφή, η οποία δεν έχει αποκρυπτογραφηθεί ακόμα. Εικάζεται ότι πρόκειται για μια φωνητική γραφή, της οποίας χαρακτηριστικό εύρημα αποτελεί ο δίσκος της Φαιστού, που ανακαλύφθηκε το 1908 στη νότια Κρήτη και χρονολογείται γύρω στα 1700 π.Χ. Μέχρι σήμερα δεν έχει αποκρυπτογραφηθεί και παραμένει η πιο μυστηριώδης αρχαία ευρωπαϊκή γραφή.

Ο δίσκος της Φαιστού.

Την ίδια περίπου περίοδο, τον 2ο π.Χ. αιώνα εμφανίστηκαν ακόμα δύο γραφές, η Γραμμική Α και η Γραμμική Β, οι οποίες ανακαλύφθηκαν στις αρχές του 1900 από τον Άγγλο αρχαιολόγο Άρθουρ Έβανς. Η Γραμμική Α, η οποία θεωρείται και πρόγονος της Γραμμικής Β, δεν έχει αποκρυπτογραφηθεί ακόμα και αποτελεί ένα από τα μεγαλύτερα μυστήρια της σύγχρονης αρχαιολογίας.

ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ :

Η Γραμμική Β αποκρυπτογραφήθηκε από τον νεαρό γλωσσολόγο-αρχιτέκτονα Michael Ventris το 1952 με τη βοήθεια του κλασσικού φιλόλογου John Chadwick.

Η αποκρυπτογράφηση της έγινε το 1952 με βάση τα ονόματα πόλεων που υπήρχαν μόνο σε πινακίδες από την Κρήτη και απέδειξε ότι την εποχή αυτή στην Κνωσσό μιλούσαν την ίδια γλώσσα (Ελληνική) που μιλούσαν και οι Αχαιοί.

Παράδειγμα Γραμμικής Β΄.

1.1.3 Η Στήλη της Ροζέτας

Η στήλη αυτή είναι μια πέτρινη στήλη που βρέθηκε στην Αίγυπτο κοντά στην πόλη Ροζέτα το 1799, από τα στρατεύματα που Ναπολέοντα. Πάνω της ήταν χαραγμένο το ένα κείμενο σε τρείς διαφορετικές γλώσσες-διαλέκτους, στα ιερογλυφικά, στα ελληνικά και σε μια ιερατική γραφή.

ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ:

Ο σπουδαίος Γάλλος μελετητής Ζαν-Φρανσουά Σαμπολιόν κατάφερε με βάση τα ονόματα των βασιλέων Πτολεμαίου και Αρσινόης που βρίσκονται στην στήλη να καταφέρει να αποκρυπτογραφήσει τα Αιγυπτιακά ιερογλυφικά.

1.1.4 Κρυπτοσύστημα του Vigenere

Αυτή η μέθοδος περιγράφηκε από τον Giovan Batisto Bellaso σε ένα βιβλίο το 1553 και αποδόθηκε στον Blaise de Vigenere.

A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Κρυπτογράφηση: Επιλέγουμε μια λέξη κλειδί. Γράφουμε την λέξη κλειδί πάνω στο μήνυμα μέχρι να το καλύψουμε. Για κάθε γράμμα της λέξης του μηνύματος βρίσκουμε το γράμμα που είναι στην τομή της στήλης που αρχίζει από αυτό και της γραμμής που αρχίζει από το αντίστοιχο γράμμα του κλειδιού.

<u>ΠΑΡΑΔΕΙΓΜΑ:</u>
Λέξη κλειδί : RELATIONS
Μήνυμα: TO BE OR NOT TO BE THAT IS THE QUESTION
Λέξη κλειδί : RELA T I ONSR ELAT I ONSRE LA T I O NSREL
Μήνυμα : TOBE O RNOTT OBETH AT IST HEQUE STION
Κρυπτοκείμενο : KSMEH ZB BLK SMEMP OGAJX SE J CS FLZSY

<u>ΑΠΟΚΡΥΠΤΟΓΡΑΦΗΣΗ:</u>

1. Γράφουμε την λέξη-κλειδί πάνω από το μήνυμα κλειδί πάνω από το μήνυμα επαναλαμβάνοντάς την μέχρι να το καλύψουμε.

2. Για κάθε γράμμα του κρυπτοκειμένου θεωρούμε την στήλη που ορίζει το αντίστοιχο γράμμα του κλειδιού και την κατεβαίνουμε μέχρι να το βρούμε.

3. Το γράμμα που ορίζει την γραμμή είναι το αντίστοιχο γράμμα του μηνύματος.

Συνέχεια παραδείγματος:
Λέξη κλειδί : RELA T IONSR ELA T I ONSRE LAT IO NSREL
Κρυπτοκείμενο: KSMEH ZB BLK SMEMP OGAJX SE J CS FLZSY
Μήνυμα : TOBE O RNOTT OBETH AT IST HEQUE STION

Στον Μεσαίωνα, η κρυπτολογία και επομένως και η κρυπτογραφία θεωρούνταν μορφή αποκρυφισμού και μαύρης μαγείας, οπότε η ανάπτυξη της ήταν πολύ περιορισμένη. Η εξέλιξη όμως της κρυπτολογίας και των μαθηματικών συνεχίζεται στον Αραβικό κόσμο. Η κοινωνία ήταν ειρηνική και εύπορη και για αυτό μπορούσε να υπάρξει αυτός ο πλούτος στις επιστήμες. Οι διοικούντες αυτής της κοινωνίας στηρίζονταν στην ασφαλή επικοινωνία που επιτυγχάνονταν μέσω της κρυπτογραφίας. Οι αξιωματούχοι προστάτευαν τα κρατικά έγγραφα με καθημερινή χρήση κρυπτογραφίας.

Οι Άραβες λόγιοι όμως ήταν πολύ καλοί όχι μόνο στο να δημιουργούν κρυπτοσυστήματα, αλλά και στο να τα σπάζουν. Αυτοί επινόησαν την κρυπτανάλυση, την επιστήμη της αποκρυπτογράφησης μηνύματος χωρίς τη γνώση του κλειδιού. Οι Άραβες κρυπταναλυτές κατάφεραν να βρουν μία μέθοδο για να σπάσουν το μονοαλφαβητικό κρυπτόγραμμα υποκατάστασης που επί αιώνες έμενε απαραβίαστο. Στην προσπάθεια τους να αποκτήσουν τις γνώσεις παλαιότερων πολιτισμών, συγκέντρωναν κείμενα όλων των σπουδαίων αρχαίων πολιτισμών και τα μετέφραζαν στα Αραβικά. Εκτός από αυτές τις μελέτες, ανέπτυξαν θρησκευτικές σπουδές. Είχαν ενδιαφέρον να καθορίσουν την χρονολογική σειρά των αποκαλύψεων και για αυτό μετρούσαν τη συχνότητα εμφάνισης των λέξεων που περιείχε κάθε αποκάλυψη. Αυτό γινόταν λόγω της θεωρίας ότι ορισμένες λέξεις έχουν εξελιχτεί σχετικά πρόσφατα και χάρη σε αυτό, τοποθετούσαν χρονολογικά τις αποκαλύψεις. Μελετούσαν επίσης την δομή των φράσεων ,των λέξεων και ανέλυαν τα επιμέρους γράμματα. Παρατήρησαν ότι ορισμένα γράμματα είναι πιο κοινά από άλλα. Αυτή η παρατήρηση οδήγησε στην πρώτη μεγάλη πρόοδο στην κρυπτανάλυση. Η παλαιότερη γνωστή περιγραφή της τεχνικής ανήκει στον επιστήμονα Αλ-Κιντί. Η θεωρία αυτή μπορεί να εξηγηθεί πιο εύκολα με το ελληνικό αλφάβητο. Μελετάμε ένα κείμενο και βλέπουμε τη συχνότητα εμφάνισης κάθε γράμματος του αλφάβητου. Στο ελληνικό αλφάβητο για παράδειγμα , πιο συχνά εμφανίζεται το α. Μελετώντας το κρυπτοκείμενο, αν πιο συχνά εμφανίζεται το χ, υποθέτουμε ότι έχει αντικαταστήσει το α. Η τεχνική αυτή ονομάζεται ανάλυση συχνότητας και δείχνει ότι δεν είναι απαραίτητο να ελέγξουμε δισεκατομμύρια πιθανά κλειδιά αρκεί να αναλύσουμε τη συχνότητα εμφάνισης χαρακτήρων σε ένα κρυπτογραφικό κείμενο. Φυσικά αυτή η μέθοδος δεν είναι δυνατό να εφαρμοστεί σε όλες τις περιπτώσεις. Ο παρακάτω πίνακας είναι ένας μέσος όρος και δεν ανταποκρίνεται επαρκώς στις συχνότητες κάθε κειμένου. Τα σύντομα κείμενα, ειδικά αυτά που έχουν κάτω από 100 χαρακτήρες τείνουν να αποκλίνουν περισσότερο από τις μέσες συχνότητες.

Η συγκεκριμένη τεχνική βέβαια απαιτεί λογική σκέψη αλλά και πονηριά, προσαρμοστικότητα, ενόραση.

ΠΙΝΑΚΑΣ ΑΝΑΛΥΣΗΣ ΣΥΧΝΟΤΗΤΩΝ

Γράμμα	Συχνότητα εμφάνισης (%)	Γράμμα	Συχνότητα εμφάνισης (%)
α	12	ν	7.9
β	0.8	ξ	0.6
γ	2	ο	9.8
δ	1.7	π	5.024
ε	8	ρ	5.009
ζ	0.5	σ	4.9
η	2.9	τα	9.1
θ	1.3	υ	4.3
ι	7.8	φ	1.2
κ	4.2	χ	1.4
λ	3.3	ψ	0.2
μ	4.4	ω	1.6

Παρότι η μέθοδος φαντάζει εντυπωσιακά απλή, είναι η βάση για πολλές τεχνικές κρυπτανάλυσης ενώ έως και τη δεκαετία του 1950 πολλές υπηρεσίες πληροφοριών βασίζονταν ακόμα σε αυτή τη μέθοδο για τη κρυπτανάλυση υποκλοπών κρυπτογραφημένων επικοινωνιών των εχθρών τους. Ωστόσο, ο Β' Παγκόσμιος Πόλεμος, μετέπειτα ο Ψυχρός Πόλεμος, και σε τεράστιο βαθμό το διαδίκτυο άλλαξαν πολλά στο τομέα της κρυπτογραφίας και της κρυπτανάλυσης. Ακόμα και σήμερα όμως, η N-γραμματική πιθανοτική ανάλυση χρησιμοποιείται από κρυπταναλυτές.

1.2 20ος Αιώνας

Η δεύτερη περίοδος τοποθετείται το πρώτο μισό του 20ου αιώνα. Περιλαμβάνει δηλαδή, τους δύο παγκόσμιους πολέμους, εξαιτίας των οποίων η κρυπτογραφία αναπτύχθηκε ραγδαία, τόσο όσο δεν είχε αναπτυχθεί τα προηγούμενα 3000 χρόνια. Αυτό συνέβη λόγω της εξαιρετικά μεγάλης ανάγκης που υπήρχε για την ασφάλεια και τη μετάδοση ζωτικών πληροφοριών μεταξύ των αντίπαλων στρατευμάτων, αλλά και την ανάγκη για αναγνώριση των στρατηγικών κινήσεων των αντιπάλων. Τα κρυπτοσυστήματα αυτής της περιόδου αρχίζουν να γίνονται πολύπλοκα, και να αποτελούνται από μηχανικές και ηλεκτρομηχανικές κατασκευές, οι οποίες ονομάζονται «κρυπτομηχανές».

Η κρυπτανάλυση τους, απαιτεί μεγάλο αριθμό προσωπικού, το οποίο εργαζόταν επί μεγάλο χρονικό διάστημα ενώ ταυτόχρονα γίνεται εξαιρετικά αισθητή η ανάγκη για μεγάλη υπολογιστική ισχύ. Παρά την πολυπλοκότητα που αποκτούν τα συστήματα κρυπτογράφησης κατά τη διάρκεια αυτής της περιόδου η κρυπτανάλυση τους είναι συνήθως επιτυχημένη.

Ο Edgar Allan Poe (1809-1849) στο κλασικό διήγημα "Το χρυσό έντομο" ("The Gold Bug") που δημοσίευσε το 1843, εξηγεί τις βασικές αρχές παραβίασης των κωδίκων και υποστηρίζει την άποψη ότι ο ανθρώπινος νους μπορεί να σπάσει οποιοδήποτε κρυπτογραφημένο κείμενο που η ανθρώπινη ευρηματικότητα μπορεί να επινοήσει. Ακόμη περιγράφει ένα σύστημα με το οποίο κάθε κρυπτογραφημένο κείμενο που προέρχεται από μια ευρωπαϊκή γλώσσα μπορεί να αποκρυπτογραφηθεί, αν έχει κρυπτογραφηθεί με αντικατάσταση, μετρώντας τη συχνότητα των γραμμάτων της γλώσσας, την τεχνική που πρώτοι συνέλαβαν οι Άραβες.

Ίσως από τα διασημότερα κρυπτογραφήματα, το σημείωμα του Zimmerman (the Zimmerman Note) ώθησε τις ΗΠΑ στον πρώτο παγκόσμιο πόλεμο. Όταν το κρυπτογράφημα αποκρυπτογραφήθηκε το 1917, οι Αμερικανοί έμαθαν ότι η Γερμανία είχε προσπαθήσει να πείσει το Μεξικό να μπει στον πόλεμο με το μέρος της, παραχωρήσεις εδαφών των ΗΠΑ στο Μεξικό.

Τον ίδιο περίπου καιρό, ο Gilbert S. Vernam της AT&T ανέπτυξε τον πρώτο πραγματικά άθραυστο κώδικα που ονομάστηκε βέβαια κρυπτόγραμμα Vernam (TheVernam Cipher). Μια ξεχωριστή ιδιότητα αυτού του κώδικα είναι η απαίτηση για ένα κλειδί με μήκος όσο και το μήνυμα που πρέπει να μεταδοθεί και το οποίο δεν επαναχρησιμοποιείται για την αποστολή άλλου μηνύματος (η κρυπτογράφηση Vernam είναι γνωστή επίσης και ως κρυπτογράφηση με μπλοκάκι μιας χρήσης (onetime-pad) από την πρακτική της προμήθειας κατασκόπων με το κείμενο-κλειδί γραμμένο σε ένα μπλοκάκι του οποίου κάθε κομμάτι χρησιμοποιείται μια φορά και μετά καταστρέφεται). Η ανακάλυψη του συστήματος αυτού δεν εκτιμήθηκε ιδιαίτερα εκείνη την εποχή, πιο πολύ επειδή δεν είχε αποδειχτεί ακόμη ότι είναι άθραυστος κώδικας και επειδή η απαίτηση για πολλά και μεγάλα κλειδιά την έκαναν μη πρακτική για γενική χρήση.

Εξαιτίας των μη πρακτικών απαιτήσεων της κρυπτογράφησης Vernam, άλλες (πιο αδύναμες) μέθοδοι συνέχισαν να χρησιμοποιούνται ευρέως. Έτσι, κατά το δεύτερο παγκόσμιο πόλεμο, οι Σύμμαχοι ήταν σε θέση να αποκρυπτογραφούν τα περισσότερα από τα μυστικά μηνύματα που στέλνονταν από τους Γερμανούς. Η εγγενής δυσκολία του σπασίματος των ολοένα και πιο περίπλοκων κρυπτογραφικών μεθόδων ήταν μάλιστα ένας από τους παράγοντες που προώθησε την ανάπτυξη των ηλεκτρονικών υπολογιστών.

1.2.1 Η κρυπτανάλυση της μηχανής ENIGMA

Η πιο διάσημη περίπτωση κρυπτανάλυσης ήταν αυτή της Μηχανής Enigma, η οποία ήταν η πρώτη συσκευή κρυπτογραφίας με εξαιρετική μέθοδο κρυπτογράφησης. Σχεδιάστηκε από το Γερμανό μηχανικό Arthur Scherbius το 1918 και χρησιμοποιήθηκε από τους Γερμανούς κατά τον Α΄ Παγκόσμιο Πόλεμο. Αποτέλεσε βασικό εξοπλισμό των γερμανικών υποβρυχίων και παράλληλα μπορούσε να μεταφέρεται με ευκολία στα πεδία μαχών. Ήταν δυνατή η παραγωγή περίπου 17 τρισεκατομμυρίων διαφορετικών κωδικοποιήσεων.

Ο Marian Rejewski, στην Πολωνία, προσπάθησε και, τελικά, παραβίασε την πρώτη μορφή του γερμανικού στρατιωτικού συστήματος Enigma (που χρησιμοποιούσε μια ηλεκτρομηχανική κρυπτογραφική συσκευή) χρησιμοποιώντας θεωρητικά μαθηματικά το 1932. Ήταν η μεγαλύτερη σημαντική ανακάλυψη στην κρυπτολογική ανάλυση της εποχής. Οι Πολωνοί συνέχισαν να αποκρυπτογραφούν τα μηνύματα που βασίζονταν στην κρυπτογράφηση με το Enigma μέχρι το 1939. Τότε, ο γερμανικός στρατός έκανε ορισμένες σημαντικές αλλαγές και οι Πολωνοί δεν μπόρεσαν να τις παρακολουθήσουν, επειδή η αποκρυπτογράφηση απαιτούσε περισσότερους πόρους από όσους μπορούσαν να διαθέσουν. Έτσι, εκείνο το καλοκαίρι μεταβίβασαν τη γνώση τους, μαζί με μερικές μηχανές που είχαν κατασκευάσει, στους Βρετανούς και τους Γάλλους.

Η ΜΗΧΑΝΗ ENIGMA.

Οι Βρετανοί συγκέντρωσαν μια ομάδα κρυπταναλυτών και μαθηματικών, με επικεφαλής τον Alan Turing, σε μια βικτωριανή έπαυλη στο Buckinghamshire που ονομαζόταν Bletchley Park. Το Bletchley Park, γνωστό και σαν «Σταθμός Χ», είναι μια περιοχή 70 χιλιόμετρα βόρεια του Λονδίνου. Αποτελούσε το καλύτερο κέντρο κρυπτανάλυσης στον κόσμο, μέχρι την «επέλαση των Αμερικανών», οι οποίοι από το 1945 και μετά, κατέλαβαν εξ εφόδου την επιστημονική και πολιτική ηγεμονία του πλανήτη. Εκεί λειτουργούσε με βρετανική ακρίβεια και σχολαστικότητα, ένα συνονθύλευμα από ευφάνταστους γλωσσολόγους, κλασικούς φιλόλογους, ιδιοφυείς μαθηματικούς, εφευρετικούς ηλεκτρονικούς, ακαταπόνητους μηχανικούς, φανατικούς λύτες σταυρόλεξων και εκκεντρικούς αξιωματικούς. Υπήρχε, ακόμη εκεί, ο πρωταθλητής σκάκι της Βρετανίας και μέλη της εθνικής ομάδας μπριτζ. Αυτό το ετερογενές ανθρώπινο μείγμα, όμως, αποκάλυψε εκπληκτικές ικανότητες και σημείωσε απίστευτες επιτυχίες στην κρυπτανάλυση.

Χρησιμοποιώντας τις πληροφορίες των Πολωνών, η ομάδα βάσισε τις προσπάθειές της στη λεγόμενη μέθοδο πιθανής λέξης. Η μέθοδος αυτή βασίζεται στο γεγονός ότι σε κάποιες περιπτώσεις μια συγκεκριμένη ακολουθία συμβόλων σχεδόν σίγουρα αντιπροσωπεύει μια γνωστή λέξη. Μαντεύοντας σωστά μερικές από τις κρυπτογραφημένες λέξεις του κρυπτοκειμένου, μπορούσαν να καθορίζουν τη συνδεσμολογία της μηχανής, δοκιμάζοντας όλες

τις πιθανές συνδεσμολογίες και προσδιορίζοντας ποια είχε ως αποτέλεσμα τα υποτιθέμενα ζευγάρια κρυπτογραφημένων-αποκρυπτογραφημένων λέξεων. Ο Turing αντιλήφθηκε ότι μόνο μια αυτόματη και σχετικά γρήγορη μηχανή θα μπορούσε να τα βγάλει πέρα με τις δοκιμές, όποτε και οδηγήθηκε στην κατασκευή ενός εξομοιωτή της μηχανής-Αίνιγμα με το όνομα Bombe. Την έλεγαν «Bombe»,, λόγω του φοβερού θορύβου που έκανε όταν λειτουργούσε! Χρησιμοποιούσε ηλεκτρομηχανική τεχνολογία, με διακόπτες και ηλεκτρονόμους.

Η «Βόμβα». Χρησιμοποιούσε ηλεκτρομηχανική τεχνολογία, με διακόπτες και ηλεκτρονόμους. Σχεδιάστηκε και κατασκευάστηκε στην πρώτη μορφή της από τους Πολωνούς, οι οποίοι, φοβούμενοι εισβολή από τη Γερμανία, προσπάθησαν με κάθε τρόπο να κρυπταναλύσουν τις επικοινωνίες τους. Λίγο πριν την έναρξη του πολέμου, τις παρέδωσαν στους Βρετανούς, με πραγματικά μυθιστορηματικό τρόπο, οι οποίοι έμειναν άναυδοι από την πρόοδο ενός μικρού και αδύναμου κράτους στον τομέα αυτό. Ήταν τουλάχιστον δέκα χρόνια πιο μπροστά, από τον υπόλοιπο κόσμο. Την πρώτη Βόμβα, την ονόμασαν «Νίκη» και αρχικά χρειαζόταν μια εβδομάδα για να σπάσει ένα κρυπτοκείμενο. Μέσα σε λίγους μήνες, ο χρόνος είχε μειωθεί σε λίγες ώρες. Συνολικά κατασκευάστηκαν 18 «Βόμβες». Στη συνέχεια, «παρελήφθη» από τις αμερικανικές ειδικές υπηρεσίες και μπήκε σε μαζική παραγωγή. Κατασκευάστηκαν περισσότερες από 100, πολύ πιο εξελιγμένες, για τις ανάγκες της NSA. Η συγκεκριμένη στη φωτογραφία, ονομάζεται AgnusDei (Αμνός του Θεού) και βρίσκεται στο μουσείο της NSA στη Βαλτιμόρη.

1.2.2 Ο «ΚΟΛΟΣΣΟΣ»

Αντίθετα, οι στρατηγικές επικοινωνίες μεταξύ της ανώτατης διοίκησης, δηλαδή του ίδιου του Χίτλερ και των στρατηγών του, διεξάγονταν με τη βοήθεια μιας πολύ εξελιγμένης μηχανής κρυπτογράφησης, της Lorenz SZ40. Αυτή η κορωνίδα της γερμανικής τεχνολογίας, ήταν ουσιαστικά, ένα τηλέτυπο, που μπορούσε ταυτόχρονα να κρυπτογραφήσει και να διαβιβάσει το κείμενο, επιτυγχάνοντας μεγάλη οικονομία χρόνου και κόπου. Μπορεί να θεωρηθεί και ως η πρώτη on-line κρυπτομηχανή.

Η κρυπτομηχανή Lorenz, ήταν θεωρητικά αδύνατον να κρυπταναλυθεί, αφού χρησιμοποιούσε τον κώδικα μιας χρήσης (one-time-pad), το μοναδικό αδιάσπαστο σύστημα κρυπτογράφησης. Εφόσον το κλειδί παράγεται με πραγματικά τυχαίο τρόπο, δηλαδή όλα τα κλειδιά είναι εξίσου πιθανά, τότε η μετάδοση είναι κρυπτογραφικά ασφαλής. Ωστόσο, οι

γερμανικές διαβιβάσεις δεν ακολουθούσαν αυτόν τον κανόνα. Επειδή η μεταφορά ταινιών με κώδικα, στο πεδίο της μάχης, είναι δύσκολη, το κλειδί το παρήγαγε επί τόπου μια μηχανή, όχι με τυχαίο τρόπο, αλλά με ψευδοτυχαίο. Οι Γερμανοί «κατασκεύαζαν» τον κώδικα μιας χρήσης, με τη βοήθεια μηχανικών συστημάτων, που δεν δημιουργούσαν τυχαίο κώδικα, αλλά ψευδοτυχαίες ακολουθίες, δηλαδή σειρές από γράμματα, που μετά από κάποιο «μήκος» επαναλαμβάνονταν. Η περίοδος της επανάληψης ήταν 1019 =10.000.000.000.000.000.000 ψηφία, που σύμφωνα με τη γερμανική διοίκηση, ήταν ασφαλής. Υπολόγιζαν όμως, χωρίς τους Άγγλους κρυπταναλυτές. Με τη βοήθεια ενός μεγάλου κρυπτογραφήματος, που διαβιβάστηκε δύο φορές με τον ίδιο κώδικα, κατάφεραν να αποκαλύψουν ένα μέρος του ψευδοτυχαίου κώδικα και στη συνέχεια να βρουν τον τρόπο δημιουργίας του.

Αυτή η εγγενής και κρίσιμη ατέλεια στη χρήση του κώδικα, έγινε αντιληπτή από τους ιδιοφυείς Άγγλους κρυπταναλυτές, οι οποίοι εργάζονταν υπό συνθήκες πρωτοφανούς μυστικότητας, στο θρυλικό Μπλίτσλεϊ Παρκ. Ο Κολοσσός σχεδιάστηκε και λειτούργησε από αυτούς τους ιδιοφυείς ανθρώπους, για την υποβοήθηση της κρυπτανάλυσης της Lorenz.

Η κρυπτομηχανή Lorenz απετέλεσε την κορυφαία πρόκληση για τους κρυπταναλυτές του Μπλίτσλεϊ. Η κρυπτανάλυση της απαιτούσε ένα κράμα πρακτικής έρευνας, συνδυαστικής ικανότητας, στατιστικής ανάλυσης και ορθής κρίσης. Οι αυτοματοποιημένοι ηλεκτρομηχανικοί βοηθοί, όπως η μηχανή «Βόμβα», δεν μπορούσαν να βοηθήσουν. Οι «βόμβες» εκτελούσαν μια μόνο συγκεκριμένη λειτουργία με μεγάλη ταχύτητα, δεν ήταν όμως αρκετά ευέλικτες, ώστε να αντιμετωπίσουν την πολυπλοκότητα της Lorenz. Οι κρυπταναλυτές ήταν αναγκασμένοι να «σπάζουν» χωρίς μηχανοποιημένη βοήθεια, τους κώδικες Lorenz, πράγμα που απαιτούσε κοπιαστική προσπάθεια εβδομάδων, οπότε και τα μηνύματα δεν ήταν πια επίκαιρα. Προσπάθησαν να περάσουν τον κώδικα σε ταινία τηλετύπου, την οποία συγχρόνιζαν με μια άλλη ταινία, που περιείχε το κρυπτοκείμενο και να παρακολουθούν το αποτέλεσμα της πρόσθεσης, μέχρις ότου ανακαλύψουν το ανοιχτό κείμενο. Η ιδέα ήταν καλή, αλλά η διαδικασία συγχρονισμού απεδείχθη ηράκλειο έργο. Εμφανίστηκε τότε ο «από μηχανής θεός», ο μαθηματικός Μαξ Νιούμαν, ο οποίος, συνδυάζοντας τις ιδέες του Τιούρινγκ για τη «λογική μηχανή καθολικής χρήσης», σχεδίασε μια μηχανή, ικανή να προσαρμόζεται με τη βοήθεια προγραμματισμού, σε διάφορα προβλήματα. Σήμερα, θα την αποκαλούσαμε «προγραμματιζόμενο υπολογιστή». Η μηχανή θα περιείχε σε «ηλεκτρονική μορφή» στη μνήμη της, τον κρυπτοκώδικα και ο συγχρονισμός θα γινόταν ηλεκτρονικά και ταχύτατα. Η ιδέα του Νιούμαν θεωρήθηκε ανεδαφική και ανέφικτη και κατέληξε στο αρχείο. Ευτυχώς, ένας ηλεκτρονικός μηχανικός, ο Τ. Φλάουερς, που δεν θεωρούσε τίποτα ακατόρθωτο, είδε τα σχέδια και αποφάσισε να αγνοήσει το σκεπτικισμό των ανωτέρων του και να προχωρήσει στην κατασκευή της μηχανής, στο ερευνητικό κέντρο των βρετανικών ταχυδρομείων! Μέσα σε δέκα μήνες, κατασκεύασε τον «Κολοσσό» και τον παρέδωσε σε λειτουργία το Δεκέμβριο του 1943. Η μηχανή αποτελείτο από 1.500 ηλεκτρονικές λυχνίες, απαιτούσε τάσεις τροφοδοσίας από +200 έως -150 V, χρησιμοποιούσε πεντακόσια τροφοδοτικά των 10 A, κατανάλωνε πάνω από 45kW και μπορούσε να εκτελέσει 100 λογικές πράξεις Boole, σε ένα δευτερόλεπτο. Η εισαγωγή δεδομένων γινόταν με τη βοήθεια ταινίας τηλετύπου, την οποία μπορούσε να «διαβάσει», με ταχύτητα 5.000 χαρακτήρων το λεπτό. Η πρώτη εκτίμηση των ειδικών, όταν την είδαν, ήταν ότι ο αναμενόμενος χρόνος ζωής της, πριν πάθει βλάβη (MTBF, Minimum Time Before Failure), θα ήταν μικρότερος από 2 λεπτά! Ήταν τόσο γρήγορη, που ακόμη και σήμερα, αν προγραμματίζαμε έναν υπολογιστή Pentium 4 (3,4GHz) να κάνει την ίδια εργασία, θα χρειαζόταν διπλάσιο χρόνο. Για πρώτη φορά στην ιστορία των ηλεκτρονικών, χρησιμοποιήθηκαν ηλεκτρονικές λυχνίες σαν διακόπτες υψηλής ταχύτητας, στη θέση των μέχρι τότε χρησιμοποιούμενων ηλεκτρονόμων. Ήταν η πρώτη μηχανή που χρησιμοποιούσε το δυαδικό αριθμητικό σύστημα, κάτι που εκείνη την εποχή φάνταζε

εξωπραγματικό, όσο η χρήση σήμερα στο Internet, σαν μοναδική γλώσσα επικοινωνίας, την αρχαία αραμαϊκή.

Συνολικά, κατασκευάστηκαν δέκα τέτοιες μηχανές, που πρόσφεραν ανεκτίμητο έργο. Μετά τον πόλεμο, ύστερα από διαταγή του Τσόρτσιλ, καταστράφηκαν σε «πολύ μικρά, μη αναγνωρίσιμα κομμάτια» και θάφτηκαν, ενώ τα σχέδια κάηκαν παρουσία του. Δύο από αυτές, όμως, όπως αποκαλύφθηκε πριν δύο χρόνια, μεταφέρθηκαν στο Αρχηγείο Κυβερνητικών Επικοινωνιών (Government Communications HeadQuarters, GCHQ) και δεν τις ξαναείδε κανείς, παρά μόνο μια ομάδα προσεκτικά επιλεγμένων ειδικών. Τέτοιο ήταν το δέος για αυτές τις μηχανές, που θεωρούσαν ότι ακόμη και η απλή αναφορά στην ύπαρξή της, θα στερούσε την Αγγλία από στρατηγικό πλεονέκτημα. Όλα έμειναν κρυφά για περισσότερο από 30 χρόνια, ενώ όσοι έλαβαν μέρος στην ανάπτυξη και χρήση τους, έμειναν στην αφάνεια . Έτσι, τα σχέδια για τον πρώτο υπολογιστή στον κόσμο, χάθηκαν για πάντα. Η μυστικότητα αυτή, είχε σαν συνέπεια να κερδίσουν άλλοι επιστήμονες τη δόξα της επινόησης του ηλεκτρονικού υπολογιστή.

Πριν λίγους μήνες, τον Ιούλιο 2004, με την ευκαιρία της συμπλήρωσης 50 ετών από την D-Day, την ημέρα της απόβασης στη Νορμανδία, έγιναν τα εγκαίνια μιας κατασκευασμένης από την αρχή μηχανής «Κολοσσός». Αρχηγός της προσπάθειας ήταν και πάλι ο μηχανικός Τ. Φλάουερς, μαζί με μια ομάδα από ενθουσιώδεις βετεράνους και ερασιτέχνες, οι οποίοι συγκρότησαν το «Colossus Rebuild Project». Χωρίς βοήθεια από το κράτος, με δικά τους χρήματα, πολύ κόπο και τον ενθουσιασμό που χαρακτηρίζει όσους πιστεύουν σε αυτό που κάνουν, επανέφεραν στη ζωή, χωρίς σχέδια και με όλα τα εξαρτήματα ειδικά κατασκευασμένα από την αρχή, την ιστορική μηχανή - πρόγονο των σύγχρονων ηλεκτρονικών υπολογιστών. Η μηχανή αυτή εκτίθεται εν λειτουργία στο μουσείο του Bletchley Park, στο Λονδίνο.

Ο ΚΟΛΟΣΣΟΣ

1.2.3 Το BLETCHLEY PARK

Το κρυπταναλυτικό κέντρο στο Bletchley αποκρυπτογραφούσε γερμανικά, ιταλικά και ιαπωνικά μηνύματα. Οι πληροφορίες που συλλέγονταν από αυτές τις τρεις πηγές, χαρακτηρίζονταν με το κωδικό όνομα ULTRA. Η Ούλτρα συνέβαλε στην καταστροφή των γερμανικών γραμμών ανεφοδιασμού στη Β. Αφρική, προειδοποίησε για την επικείμενη γερμανική εισβολή στην Ελλάδα, γεγονός που επέτρεψε στα βρετανικά στρατεύματα να αποχωρήσουν, χωρίς σημαντικές απώλειες και βοήθησε τη συμμαχική απόβαση στη Σικελία, το

1943. Το σημαντικότερο ρόλο, όμως, τον διαδραμάτισε κατά τη διάρκεια της συμμαχικής εισβολής στην Ευρώπη. Τους μήνες που προηγήθηκαν της Ημέρας D (απόβαση στη Νορμανδία), οι αποκρυπτογραφήσεις του Bletchley έδωσαν λεπτομερή εικόνα της κατανομής των γερμανικών γραμμών άμυνας, κατά μήκος της γαλλικής ακτής και άλλαξαν το σημείο απόβασης από την ακτή της Χάβρης και του Χερβούργου, στην περιοχή της Καν. Η επιτυχία ήταν τέτοια, που ο ίδιος ο Τσόρτσιλ έγραψε: « δεν νομίζω να υπήρξε ποτέ στο παρελθόν, από τους κλασικούς χρόνους μέχρι σήμερα, κάποιος πόλεμος, όπου η μία πλευρά διάβαζε συστηματικά τις σημαντικές στρατιωτικές πληροφορίες της άλλης ».

ΤΟ BLETCLEY PARK

Το BletchleyPark, γνωστό και σαν «Σταθμός Χ», βρίσκεται 70 χιλιόμετρα βόρεια του Λονδίνου. Στη μέση του πάρκου, βρισκόταν μια μεγάλη βικτοριανή έπαυλη, χτισμένη στο γοτθικό στιλ των Τιδόρ. Η έπαυλη, με τη βιβλιοθήκη της, την τραπεζαρία και την αίθουσα χορού, μεταβλήθηκε σε αρχηγείο της Κρατικής Σχολής Κωδίκων και Κρυπτογραφίας (GovernmentCode & CipherSchool), που εξελίχθηκε στο καλύτερο κέντρο κρυπτανάλυσης στον κόσμο. Ένα μείγμα από ευφάνταστους γλωσσολόγους, κλασικούς φιλόλογους, ιδιοφυείς μαθηματικούς, εφευρετικούς ηλεκτρονικούς, ακαταπόνητους μηχανικούς, φανατικούς λύτες σταυρόλεξων και εκκεντρικούς αξιωματικούς, την εθνική ομάδα μπριτζ και τον παγκόσμιο πρωταθλητή στο σκάκι, λειτουργούσε με βρετανική ακρίβεια και σχολαστικότητα, με αποτέλεσμα απίστευτες επιτυχίες στην ανάλυση των γερμανικών κρυπτοεπικοινωνιών. Γύρω από το όμορφο κτίριο, χτίστηκαν πολυάριθμα πρόχειρα ξύλινα υπόστεγα. Το Παράπηγμα 6 ειδικευόταν στις υποκλοπές των επικοινωνιών του γερμανικού στρατού, το 8 τις αποκρυπτογραφούσε, το 3 τις μετέφραζε και το 4 τις ανέλυε. Ξεκίνησε με προσωπικό 200 άτομα, αλλά μέσα σε πέντε χρόνια έφτασε να στεγάζει 7.000 ειδικούς στην κρυπτανάλυση. Αποτελεί, χωρίς αμφιβολία, ένα από τα μέρη, στα οποία γράφτηκε η σύγχρονη ιστορία της Ευρώπης - και ίσως του κόσμου.

1.2.4 Μηχανικές και ηλεκτρομηχανικές κρυπτομηχανές Before Computers

Οι αποκρυπτογραφήσεις αυτές οδήγησαν σε σημαντικές νίκες και έπαιξαν καθοριστικό ρόλο στην αίσια, για τις χώρες των Συμμαχικών Δυνάμεων, έκβαση του πολέμου. Οι συμμαχικές κρυπτομηχανές που χρησιμοποιήθηκαν στον δεύτερο παγκόσμιο πόλεμο περιλάμβαναν το βρετανικό TypeX και το αμερικανικό SIGABA. Και τα δύο ήταν ηλεκτρομηχανικά σχέδια παρόμοια στο πνεύμα με το Enigma, με σημαντικές εν τούτοις βελτιώσεις. Κανένα δεν έγινε γνωστό ότι παραβιάστηκε κατά τη διάρκεια του πολέμου. Τα στρατεύματα στο πεδίο μάχης χρησιμοποίησαν το M-209 και τη λιγότερη ασφαλή οικογένεια κρυπτομηχανών M-94. Άλλες κρυπτομηχανές που χρησιμοποιήθηκαν ευρύτατα στη διάρκεια του πολέμου, αλλά και μετά, είναι οι γερμανικές T52-Siemens, και οι ιαπωνικές Red και Purple, οι οποίες αποδείχθηκαν και οι ευκολότερες στη

διάσπαση. Όλες χρησιμοποιούν ένα σύστημα από ρότορες, για να παράγουν μία σειρά πολυαλφαβητικών αντικαταστάσεων. Τα συστήματα αυτά, αποδείχθηκαν όχι ιδιαιτέρως ασφαλή. Η διάσπασή τους, κατά κανόνα ήταν δυνατή, απαιτούσε όμως τεράστιο υπολογιστικό φόρτο και ιδιαίτερα εξειδικευμένο και υψηλού επιπέδου προσωπικό. Μόνο οι Άγγλοι και στη συνέχεια οι Αμερικανοί μπόρεσαν να ανταποκριθούν σε αυτές τις υψηλές απαιτήσεις και για αυτό η διαδρομή τους στο χώρο της κρυπτανάλυσης έμεινε στην ιστορία. Δουλεύαν υπό δύσκολες συνθήκες πίεσης και όμως είχαν καταφέρει άψογο συντονισμό και επιστημονική τελειότητα.

Οι προσπάθειες κρυπτανάλυσης εκείνης της περιόδου, οδήγησαν στην ανάπτυξη της πληροφορικής.

1.3 Η σύγχρονη Κρυπτανάλυση

Οι κρυπταναλυτές συνέβαλαν στην γέννηση του σύγχρονου υπολογιστή και συνέχισαν και μετά τον πόλεμο να χρησιμοποιούν και να αναπτύσσουν την τεχνολογία τους για να σπάζουν κρυπτογραφήματα. Με την ταχύτητα και την ευελιξία των σύγχρονων υπολογιστών μπορούσαν να δοκιμάζουν όλα τα πιθανά κλειδιά για να βρεθεί το σωστό. Οι κρυπτογράφοι επίσης εκμεταλλεύτηκαν την τεχνολογία για να δημιουργήσουν πιο περίπλοκα κρυπτογραφήματα.

Η κρυπτογράφηση μέσω υπολογιστή υπερέχει έναντι της μηχανικής για πολλούς λόγους. Καταρχάς μια μηχανολογική κρυπτογραφική μηχανή περιορίζεται από την κατασκευή της ,ενώ ο υπολογιστής μπορεί να μιμηθεί οποιαδήποτε υποθετική κρυπτογραφική μηχανή. Επίσης λειτουργούν με πολύ μεγαλύτερες ταχύτητες και μετατρέπουν τα πάντα σε δυαδικά ψηφία.

Την τελευταία δεκαετία υπάρχει ένα αυξανόμενο ενδιαφέρον στην εφαρμογή μεθόδων τεχνητής νοημοσύνης σε προβλήματα που προκύπτουν στον τομέα της κρυπτογραφίας και κρυπτανάλυσης. Αυτό συμβαίνει γιατί αυτές οι μέθοδοι είναι αποτελεσματικές στον χειρισμό πολύ δύσκολων προβλημάτων και οι αυτοματοποιημένες τεχνικές είναι πολύ σημαντικές για τον σχεδιασμό και την κρυπτανάλυση των κρυπτοσυστημάτων.

Ο Alan Turing το 1950, θεωρείται ότι είναι ο πρώτος που συνέλαβε την ιδέα της υπολογιστικής και τεχνητής νοημοσύνης. Υπέθεσε ότι οι υπολογιστές, οι οποίοι μιμούνται τις διαδικασίες του ανθρώπινου μυαλού μπορούν να αναπτυχθούν. Η υπόθεση του υπονοεί ότι ένας αρκετά μεγάλος και ικανός υπολογιστής μπορεί να φέρει εις πέρας οποιαδήποτε αποστολή και να λύσει οποιοδήποτε πρόβλημα.

Η τεχνητή νοημοσύνη στην κρυπτανάλυση περιλαμβάνει μεθόδους Machine Learning (Μηχανική Εκμάθηση) και Computational Intelligence-CI (Υπολογιστική Νοημοσύνη). Η Computational Intelligence είναι η μελέτη προσαρμοστικών μηχανισμών που επιτρέπουν σε ένα σύστημα να συμπεριφέρεται με νοημοσύνη σε πολύπλοκα και μεταβαλλόμενα περιβάλλοντα. Αυτοί οι μηχανισμοί έχουν την ικανότητα να μαθαίνουν και να προσαρμόζονται σε νέες συνθήκες έτσι ώστε ένα ή περισσότερα λογικά χαρακτηριστικά γίνονται αντιληπτά για να αφομοιωθούν από το σύστημα. Για να έχουν έξυπνη συμπεριφορά, τα CI συστήματα σχεδιάζονται συχνά έτσι ώστε να μοντελοποιούν όψεις βιολογικής και φυσικής νοημοσύνης.

Συνεπώς τα συστήματα Υπολογιστικής Νοημοσύνης είναι συνήθως υβρίδια των συστημάτων : Εξελεκτικού Υπολογισμού (Evolutionary Computation -EC), Τεχνητών Νευρωνικών Δικτύων (Artificial Neural Networks-ANN) και Ασαφή Συστήματα (Fuzzy Systems-FZ).

1.4 Εφαρμογές

Οι τεχνικές εξόρυξης δεδομένων περιλαμβάνουν και την εξόρυξη κρυπτοδεδομένων , για να βρεθούν χρήσιμα πρότυπα του κρυπτογραφήματος και το μέγεθος του κλειδιού. Θεωρείται πως τα κρυπτογραφήματα είναι τυχαία, αλλά αυτό πρακτικά δεν μπορεί να ισχύει 100% . Μπορεί να υπάρχουν κάποια πρότυπα που παράγονται στο κρυπτογράφημα , τα οποία αποθηκεύονται σε φάκελο ή ρέουν στο δίκτυο, τα οποία αν εντοπιστούν μπορούν να χρησιμοποιηθούν για να εντοπίσουμε τις αδυναμίες του κρυπτογραφήματος χρησιμοποιώντας αλγόριθμους εξόρυξης δεδομένων κρύπτο.

Κάποιες εφαρμογές που εκτελούνται είναι οι εξής :

- Classification : Εντοπίζεται η φύση και η κλάση του αλγορίθμου.
- Clustering : Ομαδοποιεί τα κρυπτογραφήματα σύμφωνα με την ομοιότητα τους για να προβλεφθεί ο αλγόριθμος και το υπόδειγμα των ομάδων
- Association rule : Αυτή η ομάδα αλγόριθμων ερευνά κανόνες για σχέσεις βασισμένες σε σχετιζόμενες παραμέτρους μαζί με ζευγάρια συσχετισμών. (αρχικό κείμενο, κρυπτογράφημα)
- Pattern discovery: Λειτουργούν σαν σκάνερ και χρησιμοποιούνται ως είσοδοι σε εργαλεία ανάλυσης υψηλού επιπέδου. Αυτές οι τεχνικές εξόρυξης κρυπτογραφημένων δεδομένων εντοπίζουν συμπεριφορές κακόβουλου λογισμικού ,κλάσεις επιθέσεων.

1.5 Ιστορικό δημοσιεύσεων

Θα γίνει μία σύντομη αναφορά σε δημοσιεύσεις ερευνών από το 2000 και μετά.

- 2006 : Δημοσίευση του Barreno (et.al) για το κατά πόσο είναι ασφαλής η μηχανική εκμάθηση. Εισήγαγε και μία ταξινόμηση διαφορετικών τύπων επιθέσεων σε τέτοιου τύπου τεχνικές και συστήματα, καθώς και μεθόδους άμυνας ,δείχνοντας ένα αναλυτικό μοντέλο της συνάρτησης επίθεσης.
- 2010: Με βάση το προηγούμενο έργο του, ο Barreno πραγματοποίησε μία πιο λεπτομερή έρευνα, επεκτείνοντας την ταξινόμηση των επιθέσεων και δείχνοντας το πως αυτές οι κλάσεις επηρεάζουν το κόστος για τον κρυπταναλυτή και τον αμυνόμενο.
- 2011: Έρευνα του Hospodar (et.al) όπου πρότεινε τη χρήση μηχανικών τεχνικών στις επιθέσεις ‘’πλαϊνού καναλιού’’. Το προτεινόμενο σύστημα χρησιμοποίησε τον αλγόριθμο Least Squares Support Vector Machine (LS-SVM) με την επίθεση να είναι η κύρια ενέργεια και με στόχο την εφαρμογή λογισμικού Advanced Encryption Standard –AES. Η μελέτη έδειξε ότι η επιλογή των παραμέτρων του αλγορίθμου επηρεάζει ισχυρά τα αποτελέσματα.
- 2012: Ο Alani εισήγαγε την χρήση νευρωνικού δικτύου σε επίθεση γνωστού κειμένου για κρυπτανάλυση. Η συγκεκριμένη επίθεση προτείνει την προσαρμογή ενός νευρωνικού δικτύου στην αποκρυπτογράφηση χωρίς τη γνώση του κλειδιού κρυπτογράφησης. Η επίθεση κατάφερε να μειώσει τον χρόνο και τα απαιτούμενα γνωστά ζευγάρια απλού κειμένου-κρυπτοκειμένου για τον DES και Triple-DES σε πολύ μεγάλο βαθμό, σε σχέση με άλλες επιθέσεις τέτοιου τύπου.
- 2013: Ο Biggio (et.al) συζήτησε για έναν τύπο επίθεσης που ονόμασε επίθεση αποφυγής (evasion attack). Η επίθεση βασίζεται στην εισαγωγή αντιπαραθετικών δεδομένων στα αρχικά δεδομένα που χρησιμοποιούνται σε ένα σύστημα μηχανικής εκμάθησης.

- 2013: Την ίδια χρονιά, Ateniese et.al, παρουσίασε μία μέθοδο όπου εκμεταλλεύονται οι ταξινομητές από τους κρυπταναλυτές για να πάρουν πληροφορίες. Η εργασία εστίασε σε στατιστικές πληροφορίες οι οποίες ακούσια ή κακόβουλα αποκαλύπτονται από τους μηχανικούς ταξινομητές.
- 2014: Lerman, Bontempi και Markowitch πρότειναν την χρήση μηχανικών μεθόδων για την βελτίωση επιθέσεων ‘’πλαϊνού καναλιού’’. Αυτές οι επιθέσεις στηρίζονται στις εκτελέσεις λογισμικού των κρυπτοσυστημάτων και υπάρχουν συγκεκριμένες παραμετρικές παραδοχές στις οποίες βασίζονται οι επιθέσεις ,που με τις προτεινόμενες μεθόδους θα χαλαρώσουν και θα ασχοληθούν με υψηλής διάστασης διανύσματα των χαρακτηριστικών.
- 2015: Conti et.al δημοσίευσε μια έρευνα αναλύοντας το δίκτυο κρυπτογραφημένων πληροφοριών σε Android.Η ανάλυση εστίαζε στον εντοπισμό της δραστηριότητας του χρήστη, παρ’ όλο που ήταν κρυπτογραφημένη. Το προτεινόμενο σύστημα πέτυχε ακρίβεια 95% στην ταυτοποίηση της δραστηριότητας του χρήστη.
- 2016: Maghrebin et.al δημοσίευσαν την έρευνα τους για τη χρήση τεχνικών βαθιάς μάθησης σε side-channel attacks. Έτσι παράγονται καλύτερα αποτελέσματα με σε επιθέσεις AES.
- 2016 : Yu et.al παρουσιάζουν μία τεχνική που μπορεί να αποτρέψει την μηχανική μάθηση να γίνει εργαλείο επίθεσης για ταυτοποιήσεις ελαφρού ελέγχου.

ΚΕΦΑΛΑΙΟ 2ο : ΚΡΥΠΤΟΓΡΑΦΙΚΟΙ ΑΛΓΟΡΙΘΜΟΙ ΔΕΣΜΗΣ

2.1 Βασική Ορολογία

Κρυπτογραφία : γενικότερα είναι η ανταλλαγή μηνυμάτων μεταξύ δύο μερών με τέτοιο τρόπο, ώστε η κατανόηση του περιεχομένου των μηνυμάτων να είναι δυνατή μόνο από τον αποστολέα και τον παραλήπτη.

Κρυπτογράφηση : (encryption) ονομάζεται η διαδικασία μετασχηματισμού ενός μηνύματος σε μία ακατανόητη μορφή με τη χρήση κάποιου κρυπτογραφικού αλγορίθμου ούτως ώστε να μην μπορεί να διαβαστεί από κανέναν εκτός του νόμιμου παραλήπτη.
Η αντίστροφη διαδικασία όπου από το κρυπτογραφημένο κείμενο παράγεται το αρχικό μήνυμα ονομάζεται αποκρυπτογράφηση (decryption).

Αρχικό κείμενο (plaintext): είναι το μήνυμα το οποίο αποτελεί την είσοδο σε μία διεργασία κρυπτογράφησης.

Κλειδί (key) :είναι ένας αριθμός αρκετών bit που χρησιμοποιείται ως είσοδος στη συνάρτηση κρυπτογράφησης.

Κρυπτογραφημένο κείμενο (ciphertext) :είναι το αποτέλεσμα της εφαρμογής ενός κρυπτογραφικού αλγόριθμου πάνω στο αρχικό κείμενο.

Κρυπτανάλυση (cryptanalysis): είναι μία επιστήμη που ασχολείται με το "σπάσιμο" κάποιας κρυπτογραφικής τεχνικής ούτως ώστε χωρίς να είναι γνωστό το κλειδί της κρυπτογράφησης, το αρχικό κείμενο να μπορεί να αποκωδικοποιηθεί. Η διαδικασία δηλαδή της ανακάλυψης του *plaintext* από το *ciphertext* χωρίς να είναι γνωστό το κλειδί κρυπτογράφησης.

Κρυπτογραφικός αλγόριθμος (cipher) :είναι η μέθοδος μετασχηματισμού δεδομένων σε μία μορφή που να μην επιτρέπει την αποκάλυψη των περιεχομένων τους από μη εξουσιοδοτημένα μέρη. Κατά κανόνα ο κρυπτογραφικός αλγόριθμος είναι μία πολύπλοκη μαθηματική συνάρτηση.

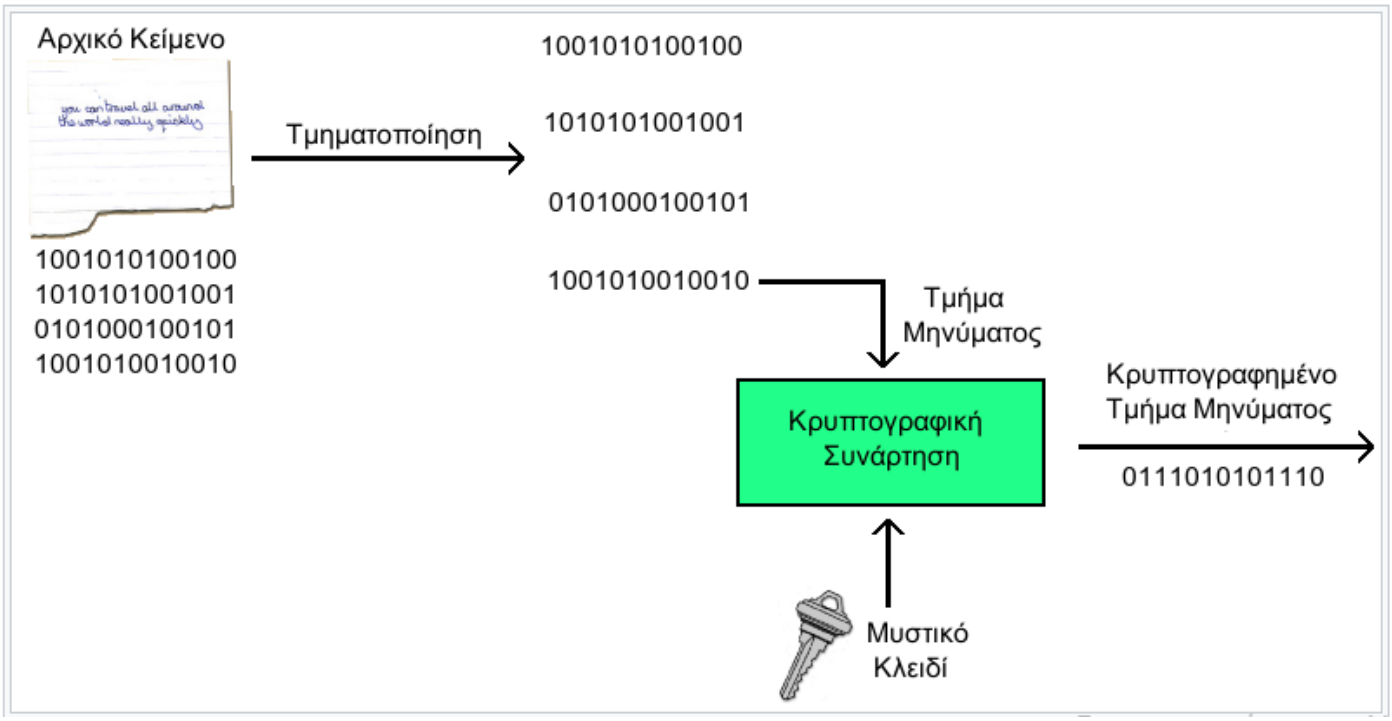
Οι κρυπτογραφικοί αλγόριθμοι (cipher) χωρίζονται σε δύο κατηγορίες : συμμετρικού κλειδιού και δημόσιου κλειδιού.

Στην περίπτωση του συμμετρικού κλειδιού ο αποστολέας και ο παραλήπτης του μηνύματος μυστικά διαλέγουν το κλειδί που θα χρησιμοποιηθεί για την κρυπτογράφηση και την αποκρυπτογράφηση. Μειονέκτημα της μεθόδου, είναι ότι πρέπει να έχουν συνεννοηθεί για το κλειδί πριν σταλθεί το μήνυμα μέσα από ασφαλές κανάλι επικοινωνίας.

Οι κρυπτογραφικοί αλγόριθμοι δημοσίου κλειδιού σχεδιάζονται με τέτοιο τρόπο έτσι ώστε το κλειδί κρυπτογράφησης είναι δημόσια διαθέσιμο και διαφέρει από το κλειδί αποκρυπτογράφησης ,το οποίο είναι μυστικό. Παρόλο που τα δύο κλειδιά φαίνονται λειτουργικά αλληλένδετα , η σύνθεση του κρυφού κλειδιού από το δημόσιο είναι υπολογιστικά δύσκολο. Έτσι χρησιμοποιώντας το δημόσιο κλειδί μπορεί ο καθένας να στείλει κρυπτογραφημένο μήνυμα, αλλά μόνο ο ιδιοκτήτης του μυστικού κλειδιού μπορεί να κάνει την αποκρυπτογράφηση.

2.2 Κρυπτογραφικοί Αλγόριθμοι Δέσμης (block ciphers)

Οι κρυπτογραφικοί αλγόριθμοι δέσμης (block ciphers) τεμαχίζουν σε τμήματα (blocks) το αρχικό κείμενο που πρόκειται να κρυπτογραφηθεί και κρυπτογραφούν κάθε τμήμα ξεχωριστά. Συνηθισμένα μεγέθη ενός τμήματος δεδομένων είναι τα 64 ή 128 bits. Η κρυπτογράφηση κάθε ενός τμήματος γίνεται χρησιμοποιώντας μία μαθηματική συνάρτηση κρυπτογράφησης και το μυστικό κλειδί. Το αποτέλεσμα της διαδικασίας κρυπτογράφησης είναι η παραγωγή ενός κρυπτογραφημένου τμήματος το οποίο στην πλειοψηφία των περιπτώσεων έχει το ίδιο μήκος με το αντίστοιχο τμήμα του αρχικού κειμένου.



Το μέγεθος του κάθε τμήματος θα πρέπει να είναι αρκετά μεγάλο ούτως ώστε να προλαμβάνονται διάφορες επιθέσεις λεξικού (dictionary attacks). Εάν το μέγεθος του κάθε τμήματος είναι μικρό, τότε μπορεί ο κρυπταναλυτής να εξετάσει ένα ζεύγος καθαρού και αντίστοιχου κρυπτογραφημένου κειμένου και να κατασκευάσει ένα λεξικό που θα αντιστοιχεί κάθε τμήμα κρυπτογραφημένου κειμένου με το αντίστοιχο τμήμα του καθαρού κειμένου. Με βάση το λεξικό αυτό, θα μπορεί στην συνέχεια να αποκρυπτογραφεί κάθε κείμενο που κρυπτογραφείται χρησιμοποιώντας το συγκεκριμένο κλειδί.

Η διαδικασία της αποκρυπτογράφησης είναι η αντίστροφη της διαδικασίας κρυπτογράφησης, μόνο που στην περίπτωση αυτή χρησιμοποιείται η συνάρτηση αποκρυπτογράφησης αντί της κρυπτογραφικής συνάρτησης.

Ένα block cipher είναι μία συνάρτηση, συνεπώς, που μετατρέπει n-bit κομμάτια , blocks, απλού κειμένου σε n-bit blocks κρυπτογραφήματος, όπου n είναι ένα επιλεγμένο μήκος block. Η συνάρτηση παραμετροποιείται από ένα k-bit κλειδί K , το οποίο λαμβάνει τιμές από ένα υποσύνολο Ķ ,*key space,* από το σύνολο όλων των k-bit διανυσμάτων. Η συνάρτηση πρέπει να είναι αναστρέψιμη για να επιτρέπει μοναδική αποκρυπτογράφηση.

Συνάρτηση: $E : V_n \times Ķ \rightarrow V_n$,τέτοια ώστε για κάθε κλειδί $K \in Ķ$ και απλό κείμενο P ,E(P,K), είναι μία αντιστρέψιμη συνάρτηση, η συνάρτηση κρυπτογράφησης. Ορίζουμε C= E (P,K) το κρυπτογράφημα που προκύπτει από την κρυπτογράφηση του P συμφώνως K.

Ένα επαναλαμβανόμενο block-cipher είναι ένα block cipher βασισμένο σε ακολουθία r επαναλήψεων μιας συνάρτησης ,της *round function.*Κάθε επανάληψη ονομάζεται *round* και το κρυπτοσύστημα ονομάζεται *r-round* κρυπτοσύστημα. Οι παράμετροι της είναι οι εξής : αριθμός rounds *r,* μέγεθος bit του block *n,* και το μέγεθος *k* του κλειδιού K ,από το οποίο r υπο-κλειδιά K_i (roundkeys) διαχωρίζονται. Αυτά τα ''υποκλειδιά'' (*round keys*) K_i υπολογίζονται με τον βασικό αλγόριθμο προγραμματισμού key scheduling algorithm.

2.2.1 S-boxes

Η round function συνήθως βασίζεται σε αντιστοιχίσεις αντικατάστασης, τα *S-boxes.* Τα S-boxes είναι βασικό συστατικό των αλγόριθμων συμμετρικού κλειδιού που πραγματοποιούν την υποκατάσταση. Είναι μη γραμμικές αντιστοιχίσεις και συνήθως είναι το μόνο μη γραμμικό μέρος του κρυπτοσυστήματος , ωστόσο η ασφάλεια του κρυπτοσυστήματος βασίζεται σε μεγάλο βαθμό σε αυτά. Λόγω της σπουδαιότητας του ρόλου τους τα θέματα μηχανικής του σχεδιασμού και κατασκευής των S-boxes λαμβάνουν ιδιαίτερη προσοχή.
Ένα S-box δέχεται έναν αριθμό εισερχόμενων bits m και τα μετατρέπει σε εξερχόμενα bit n ,τα οποία δεν είναι απαραίτητα ίσα με m. Ένα m *n S-box μπορεί να παρουσιαστεί ως πίνακας αναζήτησης με 2^m λέξεις από n bits η καθεμία. Συνήθως χρησιμοποιούνται σταθεροί πίνακες ,όπως στον DES ,αλλά σε μερικά κρυπτογραφήματα οι πίνακες παράγονται δυναμικά από το κλειδί. (πχ. Blowfish αλγόριθμο)

S_5		Middle 4 bits of input															
		0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Outer bits	00	0010	1100	0100	0001	0111	1010	1011	0110	1000	0101	0011	1111	1101	0000	1110	1001
	01	1110	1011	0010	1100	0100	0111	1101	0001	0101	0000	1111	1010	0011	1001	1000	0110
	10	0100	0010	0001	1011	1010	1101	0111	1000	1111	1001	1100	0101	0110	0011	0000	1110
	11	1011	1000	1100	0111	0001	1110	0010	1101	0110	1111	0000	1001	1010	0100	0101	0011

Πίνακας με DES με είσοδο 6-bit σε εκροή 4-bit.

2.3 Feistel Cipher.

Στην κρυπτογραφία, ένα Feistel cipher είναι μια συμμετρική δομή που χρησιμοποιείται στην κατασκευή μπλοκ κρυπτογράφησης, που πήρε το όνομά του από τον Γερμανό-γεννημένο φυσικό και κρυπτογράφο Horst Feistel που έκανε πρωτοποριακή έρευνα ενώ εργαζόταν για την IBM. Είναι επίσης κοινώς γνωστό ως δίκτυο Feistel.

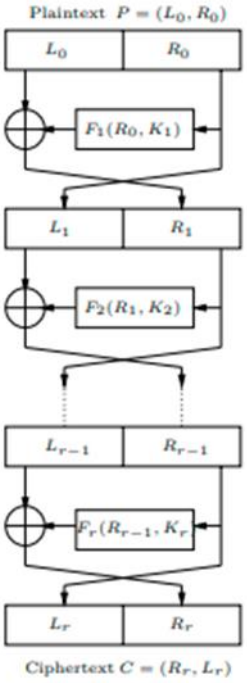
Είναι ένα επαναλαμβανόμενο block cipher βασισμένο στις round functions. Μετασχηματίζει ένα n-bit απλού κειμένου P σε κρυπτοκείμενο C , μέσα από ένα προκαθορισμένο αριθμό γύρων r. Σε ένα Feistel cipher η τρέχουσα n-bit λέξη διαιρείται σε n/2 bit parts,το αριστερό L_i και το δεξί Ri. Η επανάληψη r έχει ως εξής :

$L_i = R_i - 1$

$R_i = L_{i-1} \oplus F(R_{i-1}, K_i)$, όπου K_i είναι το δευτερεύον κλειδί που χρησιμοποιείται στον i_{th} γύρο και F είναι μία αυθαίρετη round συνάρτηση. Ο αριθμός των γύρων είναι συνήθως μονός αριθμός. Η εκροή μιας κρυπτογράφησης feistel είναι (R_r, L_r) . Όταν πραγματοποιηθεί ο τελευταίος γύρος ,τα δύο μισά ανταλλάσσονται.

Ένα χαρακτηριστικό του κρυπτογραφήματος Feistel είναι ότι η συνάρτηση αποκρυπτογράφησης είναι ίδια με αυτή της κρυπτογράφησης, αλλά τα δευτερεύοντα κλειδιά και

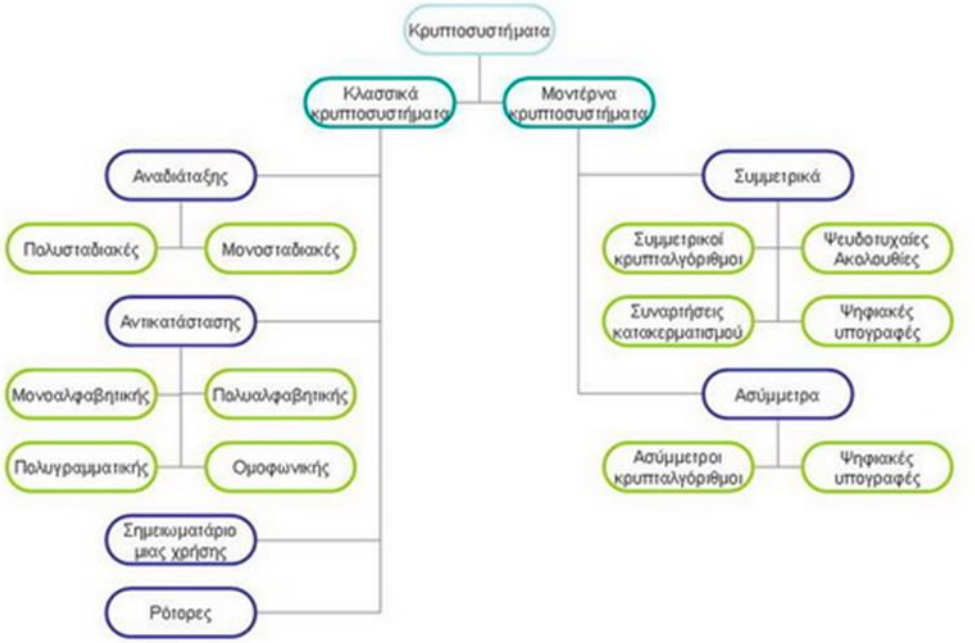
οι συναρτήσεις round είναι σε αντίστροφη σειρά. Αυτά τα χαρακτηριστικά την κάνουν μία ελκυστική επιλογή τόσο για τις συσκευές όσο και για το λογισμικό.



Η διαδικασία κρυπτογράφησης με Feistel.

2.4 Data Encryption Standard (DES)

Δύο είναι οι κατηγορίες κρυπτοσυστημάτων : τα κλασσικά και τα μοντέρνα , τα οποία χωρίζονται σε συμμετρικά και ασύμμετρα. Θα ασχοληθούμε με διάφορα θέματα μοντέρνων κρυπτοσυστημάτων.



Όπως ειπώθηκε και στην εισαγωγή, συμμετρικό κρυπτοσύστημα είναι το σύστημα εκείνο το οποίο χρησιμοποιεί κατά τη διαδικασία της κρυπτογράφησης ή αποκρυπτογράφησης ένα κοινό κλειδί. Η ασφάλεια αυτών των αλγορίθμων βασίζεται στη μυστικότητα του κλειδιού. Τα

συμμετρικά κρυπτοσυστήματα προϋποθέτουν την ανταλλαγή του κλειδιού μέσα από ένα ασφαλές κανάλι επικοινωνίας ή μέσα από την φυσική παρουσία των προσώπων. Αυτό το χαρακτηριστικό καθιστά δύσκολη την επικοινωνία μεταξύ απομακρυσμένων ατόμων. Σε αυτή την κατηγορία χρησιμοποιούνται block ciphers.

Ένας από τους πιο ευρέως χρησιμοποιούμενους Feistel κρυπτογραφικούς αλγόριθμους δέσμης είναι ο Data Encryption Standard (DES). Ο DES είναι το αποτέλεσμα της συνεργασίας της κυβέρνησης των ΗΠΑ και της IBM το 1970. Είναι ένας συμμετρικός αλγόριθμος , δηλαδή τα μέρη που ανταλλάσσουν πληροφορίες κατέχουν το ίδιο κλειδί. Ο DES επεξεργάζεται κομμάτια απλού κειμένου n=64 bits και παράγει block κρυπτοκειμένου 64-bit, με κλειδί *k* = 64 bits , 8 εκ των οποίων μπορούν να χρησιμοποιηθούν ως *parity bits.*

Το απλό κείμενο χωρίζεται σε αριστερό και δεξί κομμάτι των 32 bits το καθένα. Το κύριο μέρος της round συνάρτησης είναι η F συνάρτηση, η οποία δουλεύει στο αριστερό κομμάτι των δεδομένων, χρησιμοποιώντας ένα δευτερεύων κλειδί 48 bit και 8 (6 ως 4 bits) S-boxes. Τα 32 bit εκροής της F συνάρτησης γίνονται XORed με το αριστερό μέρος μισό των δεδομένων και τα δύο μισά ανταλλάσσονται.

$Li = Ri{-}1 \; \kappa\alpha\iota \; Ri = Li{-}1 \oplus f(Ri{-}1, Ki)$

2.5 Επιθέσεις Κρυπτανάλυσης για Feistel ciphers.

Δύο από τις πιο δυνατές επιθέσεις για Feistel κρυτπογραφήματα βασίζονται στην εκμετάλλευση συγκεκριμένων αδυναμιών των S-boxes του κρυπτοαλγόριθμου - στόχου. Αυτές οι επιθέσεις κρυπτανάλυσαν με επιτυχία τον DES και είναι οι : *Linear Cryptanalysis* (Γραμμική Κρυπτανάλυση) και η *Differential Cryptanalysis* (Διαφορική Κρυπτανάλυση).

2.5.1 Differential Cryptanalysis

Η Differential Cryptanalysis (Διαφορική Κρυπτανάλυση) είναι μία επίθεση βασισμένη στην επιλογή απλού κειμένου (chosen plaintext attack) ,δηλαδή ο αντίπαλος έχει προσωρινή πρόσβαση στην συνάρτηση κρυπτογράφησης και μπορεί να επιλέξει μερικά απλά κείμενα και να κατασκευάσει τα αντίστοιχα κρυπτογραφήματα. Η Differential Cryptanalysis (DC) αναλύει την επίδραση συγκεκριμένων διαφορών σε ζευγάρια απλού κειμένου πάνω σε διαφορές των κρυπτογραφημένων ζευγαριών που δημιουργούνται. Αυτές οι διαφορές μπορούν να χρησιμοποιηθούν για να βρεθούν οι πιθανότητες των πιθανών κλειδιών και να ταυτοποιηθούν τα bits του κλειδιού που χρησιμοποιήθηκαν στην διαδικασία κρυπτογράφησης. Αυτή η μέθοδος συνήθως λειτουργεί για έναν αριθμό από ζεύγη απλών κειμένων που έχουν συγκεκριμένη διαφορά και βασίζεται μόνο στα αποτελέσματα των ζευγαριών κρυπτογραφημάτων. Για κρυπτοσυστήματα παρόμοια με DES , η διαφορά είναι επιλεγμένη ως μία σταθερή XORed αξία από τα δύο απλά κείμενα.

Για να εντοπίσει το πιο πιθανό κλειδί , η Differential Cryptanalysis επιστρατεύει χαρακτηριστικά (*characteirtsics*). Κάθε ζευγάρι κρυπτογραφημένων κειμένων σχετίζεται με την XOR αξία των δύο απλών κειμένων του, την XOR αξία των κρυπτοκειμένων του , τις XOR αξίες των εισροών κάθε γύρου στις δύο κρυπτογραφημένες εκτελέσεις και τις XOR αξίες των εκροών κάθε γύρου στις δύο κρυπτογραφημένες εκτελέσεις. Αυτές οι XOR αξίες δημιουργούν ένα r-round χαρακτηριστικό. Ένα r-round χαρακτηριστικό είναι μία πλειάδα $\Omega = (\Omega_P, \Omega_\Lambda, \Omega_C)$,όπου Ω_P και Ω_C είναι n bit αριθμοί και Ω_Λ είναι η μία λίστα από r στοιχεία $\Omega_\Lambda = (\Lambda_1, \Lambda_2, \ldots\ldots, \Lambda_r)$,κάθε ένα από τα

ζευγάρια είναι της μορφής $\Lambda_i = (\lambda^i_I, \lambda^i_O)$ όπου λ^i_I και $\lambda_O{}^i$ είναι n/2 bit αριθμοί και n είναι το μέγεθος block του κρυπτοσυστήματος. Ένα χαρακτηριστικό ικανοποιεί τις ακόλουθες απαιτήσεις :

(a) λ_I^1 is the right half of Ω_P,
(b) λ_I^2 is the left half of $\Omega_P \oplus \lambda_O^1$,
(c) λ_I^r is the right half of Ω_C,
(d) λ_I^{r-1} is the left half of $\Omega_C \oplus \lambda_O^r$, and
(e) for every i, $2 \leqslant i \leqslant r-1$, it holds that $\lambda_O^i = \lambda_I^{i-1} \oplus \lambda_I^{i+1}$.

Σε κάθε χαρακτηριστικό αναθέτεται η πιθανότητα ενός τυχαίου ζευγαριού με το επιλεγμένο απλό κείμενο XOR ,Ω_P ,έχοντας τις XOR αξίες του γύρου , Λ_i και το κρυπτοκείμενο XOR, Ω_C καθορισμένα στο χαρακτηριστικό. Κάθε χαρακτηριστικό επιτρέπει την έρευνα για ένα συγκεκριμένο σύνολο bits στο δευτερεύον κλειδί του τελευταίου γύρου: για τα bits που εισάγονται σε συγκεκριμένο S-box, εξαρτώμενα από το επιλεγμένο χαρακτηριστικό. Τα πιο χρήσιμα χαρακτηριστικά είναι αυτά που έχουν τη μέγιστη πιθανότητα και τον μέγιστο αριθμό bit δευτερεύοντος κλειδιού των οποίων οι εμφανίσεις μπορούν να μετρηθούν.

Η Διαφορική Κρυπτανάλυση είναι μία στατιστική μέθοδος που σπάνια αποτυγχάνει. Ήταν η πρώτη θεωρητική κρυπτανάλυση για DES που απαιτούσε ,κατά μέσο όρο, λιγότερα βήματα από την επίθεση ωμής βίας, πχ δοκιμή 2^{56} = 72 057 594 037 927 936 πιθανά κλειδιά. Ακόμη και αν το νούμερο φαίνεται απαγορευτικό, μία επίθεση ωμής βίας σε DES 56-bit , χρησιμοποιώντας τεχνολογικά επίπεδα περασμένων δεκαετιών, επιτυχώς ξεκίνησε. Ένα ειδικά σχεδιασμένο μηχάνημα υπολογιστή μαζί με το κατάλληλο λογισμικό , σχεδιασμένο και κατασκευασμένο από το Cryptography Research , Advanced Wireless Technologies και την EEF (Electronic Frontier Foundation) έφτασε μία τιμή βασικών αναζητήσεων περίπου 90 δις. κλειδιών το δευτερόλεπτο. Αυτό το πρωτότυπο που ονομάζεται Deep Crack, περιέχει 29 πίνακες που ο καθένας διαθέτει 64 ειδικά σχεδιασμένα τσιπ.

Αυτή η επιτυχία αναζήτησης κλειδιού οδήγησε στον προσδιορισμό του κλειδιού στην πρόκληση του RSA DES (αξίας $10.000) μετά από 56 ώρες προσπαθειών τον Ιούλιο του 1998. Επιπλέον το κόστος παράμενε σε σχετικά χαμηλό επίπεδο, κάτω από $250.000 (πολύ χαμηλότερα σήμερα) το οποίο δίνει στο κατόρθωμα αυτό ακόμη μεγαλύτερη σημασία και σκέψη για την ασφάλεια του DES των 56-bit.

Ωστόσο, το National Institute of Standards and Technology (NIST) είχε διεξάγει το 1997 διεθνή διαγωνισμό για ,δεχόμενο προτάσεις για αυτό που θα αντικαταστήσει τον DES. Ο νικητής ήταν ο AES και αναμένεται να αποκρούει επιθέσεις για μία περίοδο τουλάχιστον 30 χρόνων, όπως επισήμανε ο διευθυντής ασφαλείας του NIST. Ο AES έγινε το κυβερνητικό πρότυπο και χρησιμοποιήθηκε και σε ιδιωτικές εταιρείες (σε εκδόσεις χωρίς δικαιώματα). Το 1998 το NIST ανακοίνωσε την αποδοχή 15 υποψήφιων αλγόριθμων (στον πρώτο γύρο της διαδικασίας) και κατέφυγε στην κρυπτογραφική κοινότητα για την έρευνα της απόδοσης και της ασφάλειας τους. Αφού μελετήθηκαν τα αποτελέσματα, σε δεύτερη φάση, το NIST επέλεξε 5 φιναλίστ. Ανάμεσα σε αυτούς, ο Rijndael , προτεινόμενος από τους Daemen και Rijndael επιλέχθηκε ως ο νέος DES.

Σε τρίτη επανεξέταση , το NIST κατέληξε στο ότι ο Rijndael κρυπταλγόριθμος πρέπει να γίνει ο νέος AES. Έκτοτε έχουν προταθεί πολλές επιθέσεις ,αλλά καμία με καταστροφικό αποτελέσματα.

2.5.2 <u>Διατύπωση προβλήματος.</u>

Για την διαφορική κρυπτανάλυση του DES μειωμένου σε τέσσερις γύρους, οι Biham και Shamir χρησιμοποιούν ένα χαρακτηριστικό μίας επανάληψης (round) με πιθανότητα 1 και στο

πρώτο βήμα η DC παράγει 42 bits του δευτερεύοντος κλειδιού του τελευταίου γύρου. Στην περίπτωση που τα δευτερεύοντα κλειδιά υπολογίζονται με DES αλγόριθμο προγραμματισμού κλειδιών , τα 42 bits που δίνει η DC είναι ουσιαστικά bit κλειδιών των 56 bit του κλειδιού και υπολείπονται άλλα 14.Μία πρόταση για να βρεθούν είναι να δοκιμαστούν και οι 2^{14} πιθανότητες αποκρυπτογράφησης των δοσμένων κρυπτοκειμένων, χρησιμοποιώντας τα κλειδιά που προκύπτουν. Το σωστό κλειδί θα ικανοποιεί η XOR αξία του γνωστού κειμένου για όλα τα ζευγάρια που χρησιμοποιήθηκαν από τη DC. Οι υπόλοιπες 2^{14} -1 τιμές του κλειδιού έχουν μόνο 2^{-64} πιθανότητα να ικανοποιήσει τη συνθήκη των ζευγών.

Αντί για επίθεση ωμής βίας για την εύρεση των υπόλοιπων bits, διαμορφώνουμε το πρόβλημα ως ένα πρόβλημα βελτιστοποίησης. Θεωρούμε κάθε ένα από τα bits που ψάχνουμε ως συστατικό ενός διανύσματος 14 διαστάσεων. Κάθε διάνυσμα αναπαριστά μία πιθανή λύση του προβλήματος. Υποθέτουμε ότι τα σωστά 42 bits κλειδιού που βρέθηκαν από την DC προτάθηκαν να χρησιμοποιήσουν np ζευγάρια. Μπορούμε να χρησιμοποιήσουμε αυτά τα ζευγάρια για να αξιολογήσουμε τις πιθανές λύσεις που δίνει η μέθοδος βελτιστοποίησης. Ειδικότερα, για κάθε πιθανή λύση X_i , προτεινόμενη από τον αλγόριθμο βελτιστοποίησης, κατασκευάζουμε τα 56 bits του κλειδιού , χρησιμοποιώντας τα 42 bits που είναι γνωστά από την DC και τα 14 συστατικά της X_i σε σωστή σειρά. Με το κλειδί που προκύπτει αποκρυπτογραφούμε τα np κρυπτογραφημένα ζευγάρια που χρησιμοποιήθηκαν από την DC και μετράμε τον αριθμό των αποκρυπτογραφημένων ζευγαριών που ικανοποιούν την XOR τιμή του γνωστού απλού κειμένου, που ονομάζουμε cnp_{Xi} . Επομένως, η συνάρτηση αξιολόγησης f είναι η διαφορά μεταξύ της επιθυμητής εκροής np και της πραγματικής εκροής np,

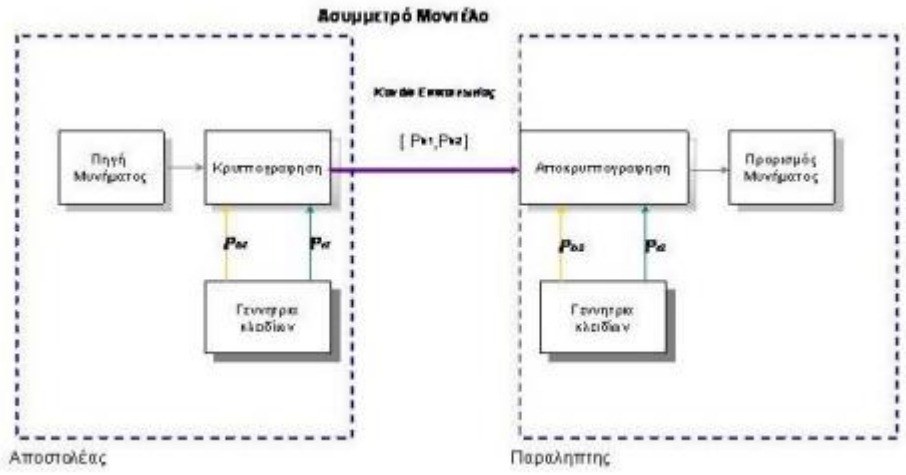
$f(X_i)= np-cnp_{Xi}$

Το ολικό ελάχιστο της συνάρτησης f είναι 0 και ο ολικός ελαχιστοποιητής που δίνεται είναι το πραγματικό κλειδί με πιθανότητα $P= 1-2^{-64}$.

2.6 Κρυπτογραφικά σχήματα δημοσίου κλειδιού

Το ασύμμετρο κρυπτοσύστημα ή κρυπτοσύστημα δημοσίου κλειδιού (Κρυπτογράφηση Δημόσιου Κλειδιού) αποτελεί τη νεότερη μορφή κρυπτογραφίας και δημιουργήθηκε για να καλύψει την αδυναμία μεταφοράς κλειδιών που παρουσίαζαν τα συμμετρικά συστήματα. Εμφανίστηκε για πρώτη φορά το 1976 από τους Diffie και Hellman και βασίζεται στην μαθηματική σχέση των κλειδιών κρυπτογράφησης και αποκρυπτογράφησης, τα οποία πλέον δεν ταυτίζονται. Γι' αυτό έχει δυο είδη κλειδιών, ένα ιδιωτικό και ένα δημόσιο. Το δημόσιο είναι διαθέσιμο σε όλους ενώ το ιδιωτικό είναι μυστικό. Η βασική σχέση μεταξύ τους είναι: ό,τι κρυπτογραφεί το ένα, μπορεί να το αποκρυπτογραφήσει μόνο το άλλο, ενώ παρά το γεγονός ότι τα κλειδιά σχετίζονται μαθηματικά, δεν υπάρχει τρόπος να υπολογιστεί το ιδιωτικό με βάση το δημόσιο. Οι δυνατότητες της ασύμμετρης κρυπτογραφίας οδήγησαν στη δημιουργία των ψηφιακών υπογραφών και ακολούθως στην ανάπτυξη της Υποδομής Δημόσιου Κλειδιού (Public Key Infrastructure) και στα Ψηφιακά πιστοποιητικά.

Η κρυπτογραφία δημοσίου κλειδιού συνδέεται στενά με έναν αριθμό δύσκολων και περίπλοκων μαθηματικών προβλημάτων από τους τομείς της υπολογιστικής άλγεβρας , την θεωρία αριθμών την πιθανολογική θεωρία, την μαθηματική λογική, την άλγεβρα γεωμετρίας και την πολυπλοκότητα Διοφαντικών εξισώσεων. Τέτοια προβλήματα είναι η παραγοντοποίηση, ο διακριτός λογάριθμος και άλλοι.



Τα κρυπτοσυστήματα βασίζονται στην υπόθεση ότι αυτά τα προβλήματα είναι υπολογιστικά μη ανιχνεύσιμα, στην αίσθηση ότι ο υπολογισμός τους δεν μπορεί να ολοκληρωθεί σε πολυωνυμικό χρόνο.

Μερικοί χαρακτηριστικοί ασύμμετροι κρυπταλγόριθμοι είναι οι εξής: RSA, DSA, Paillier, Πρωτόκολλο Diffie-Hellman, Πρότυπο El Gamal ή αλλιώς Υπογραφή El Gamal, Κρυπτογραφία ελλειπτικών καμπύλων (ECC).

2.6.1 Discrete Logarithm Problem

Το Discrete Logarithm Problem (DLP) συνοψίζεται στην ανάπτυξη ενός ικανού αλγόριθμου για την εύρεση ενός ακεραίου x που να ικανοποιεί την σχέση: $a^x = \beta$,όπου ο α είναι ένα σταθερό αρχικό στοιχείο ενός πεπερασμένου συνόλου F_q (πχ α είναι η γεννήτρια πολλαπλασιαστικού γκρουπ F^*_q του F_q) και β είναι ένα μη μηδενικό στοιχείο του πεδίου. Υποθέτουμε ότι x είναι ο μικρότερος μη αρνητικός ακέραιος με $a^x = \beta$.Έπειτα ,το x το ονομάζουμε (δείκτη) index, ή διακεκριμένο λογάριθμο του β. Στην ειδική περίπτωση ενός πεπερασμένου συνόλου Z_p μιας αρχικής εντολής p ,μία αρχική ρίζα g modulo p επιλέγεται. Αν το u είναι ο μικρότερος μη αρνητικός ακέραιος με:
$g^u \equiv h \pmod p$ τότε ο u καλείται (δείκτης) index, ή διακεκριμένος λογάριθμος του h.

Η ασφάλεια πολλών κρυπτοσυστημάτων δημοσίου και συμμετρικού κλειδιού και συγκεκριμένα το πρωτόκολλο Diffie Hellman, το κρυπτοσύστημα δημοσίου κλειδιού El Gamal και οι Ηλεκτρονικές υπογραφές βασίζονται στο γεγονός ότι το DLP είναι υπολογιστικά μη ανιχνεύσιμο.

2.6.2 Το πρόβλημα του κλειδιού DIFFIE HELLMAN (DHP)

Το πρωτόκολλο των Ντίφι-Χέλμαν παρουσιάστηκε το 1976 από τους Γουίτφιλντ Ντίφι και Μάρτιν Χέλμαν. Πριν από τη δημιουργία αυτού κάθε κρυπτογραφική τεχνική βασιζόταν σε κάποιο προσυμφωνημένο κλειδί. Το συγκεκριμένο πρωτόκολλο είναι το πρώτο που προτάθηκε ώστε να επιτρέπει σε δυο οντότητες, χωρίς προηγούμενη επικοινωνία, να ανταλλάξουν ένα κοινό κλειδί μέσω ενός μη ασφαλούς διαύλου επικοινωνίας. Η πρωτότυπη εφαρμογή του πρωτοκόλλου χρησιμοποιεί την πολλαπλασιαστική ομάδα των ακεραίων modulo p, όπου p είναι πρώτος αριθμός και g είναι γεννήτορας της πολλαπλασιαστικής ομάδας mod p.

Το a είναι ένα καθορισμένο αρχικό στοιχείο ενός πεπερασμένου συνόλου Fq : x,y που ικανοποιεί 0≤ x,y ≤ q-2 , δηλώνοντας τα ιδιωτικά κλειδιά των δύο χρηστών , και $\beta=\alpha^{x}$, $\gamma= \alpha^{y}$ αναπαριστούν τα αντίστοιχα δημόσια κλειδιά. Έπειτα, το πρόβλημα συνοψίζεται στον υπολογισμό του a^{xy} από το β και το γ, όπου α^{xy} είναι το συμμετρικό κλειδί για την μυστική επικοινωνία μεταξύ των δύο χρηστών. Η ειδική περίπτωση του DHP είναι όταν β=γ. Ο όρος DHP Mapping αναφέρεται στο $\beta=\alpha^{x} \rightarrow \alpha^{x2}$

DIFFIE- HELLMAN MAPPING PROBLEM (DHMP)

Αυτό το πρόβλημα προκύπτει από το DHP problem . Τα δύο προβλήματα είναι υπολογιστικά ίσα, η σχέση είναι : $a^{x2}\ a^{y2}\ a^{2xy} = a^{(x+y)2}$ και ο υπολογισμός του a^{xy} από το a^{2xy} είναι εφικτός (τετραγωνικές ρίζες σε καθορισμένα σύνολα)

Factorization Problem

Το πρόβλημα παραγοντοποίησης συνδέεται με τα κρυπτοσυστήματα RSA. Η ασφάλεια του συστήματος βασίζεται στην υπολογιστική μη ανίχνευση της παραγοντοποίησης ενός θετικού ακεραίου N=p*q, όπου p και q είναι διακριτοί περιττοί πρώτοι αριθμοί. Η παραγοντοποίηση του N είναι ίση με τον καθορισμό του ø (N) από N , όπου ø (N) = (p-1) x (q-1). Άπειρες τεχνικές έχουν προταθεί για επιλύσουν τα παραπάνω προβλήματα.

Elliptic Curve based cryptosystems

Τα κρυπτοσυστήματα που βασίζονται στις ελλειπτικές καμπύλες προτάθηκαν ως μία εναλλακτική στα συμβατικά κρυπτοσυστήματα δημοσίου κλειδιού. Το κύριο πλεονέκτημα τους είναι ότι έχουν μικρότερες παραμέτρους (σε όρους bits). Αυτό συμβαίνει λόγω της αυξανόμενης δυσκολίας του Elliptic Curve Discrete Logarithm Problem (ECDLP) ,το οποίο αποτελεί το υποκείμενο μαθηματικό πρόβλημα. Το ECDLP απαιτεί περισσότερο χρόνο για να λυθεί από το αντίστοιχο του, πρόβλημα με ορισμένο πεδίο , το Discrete Logarithm Problem (DLP). Η ασφάλεια τους βασίζεται στο ότι δεν μπορούν να λυθούν σε πολυωνυμικό χρόνο.

Μια ελλειπτική καμπύλη σε ένα πρωταρχικό πεπερασμένο πεδίο F_p όπου p >3 και πρώτος αριθμός, συμβολίζεται $E(F_p)$ και καθορίζεται ως το σύνολο όλων των ζευγαριών $(x,y) \in F_p$ που ικανοποιεί την ισότητα $y^3 = x^3 + ax + b$, όπου $a,b \in F_p$,με τον περιορισμό $4a^3 + 27b^2 \neq 0$. Αυτά τα σημεία, μαζί με ένα ειδικό σημείο Ὸ , το λεγόμενο σημείο στο άπειρο (point at infinity), και κατάλληλα καθορισμένα σημεία από μία λειτουργεία προσθήκης σημείων ,σχηματίζουν μία *Αβελιανή ομάδα.*

ΚΕΦΑΛΑΙΟ 3ο: ΜΕΘΟΔΟΙ ΤΗΣ ΥΠΟΛΟΓΙΣΤΙΚΗΣ ΝΟΗΜΟΣΥΝΗΣ

Ο Alan Turing το 1950, θεωρείται ότι είναι ο πρώτος που συνέλαβε την ιδέα της υπολογιστικής και τεχνητής νοημοσύνης. Υπέθεσε ότι οι υπολογιστές, οι οποίοι μιμούνται τις διαδικασίες του ανθρώπινου μυαλού μπορούν να αναπτυχθούν. Η υπόθεση του υπονοεί ότι ένας αρκετά μεγάλος και ικανός υπολογιστής μπορεί να φέρει εις πέρας οποιαδήποτε αποστολή και να λύσει οποιοδήποτε πρόβλημα.

Η τεχνητή νοημοσύνη στην κρυπτανάλυση περιλαμβάνει μεθόδους Machine Learning (Μηχανική Εκμάθηση) και Computational Intelligence-CI (Υπολογιστική Νοημοσύνη). Η Computational Intelligence είναι η μελέτη προσαρμοστικών μηχανισμών που επιτρέπουν σε ένα σύστημα να συμπεριφέρεται με νοημοσύνη σε πολύπλοκα και μεταβαλλόμενα περιβάλλοντα. Αυτοί οι μηχανισμοί έχουν την ικανότητα να μαθαίνουν και να προσαρμόζονται σε νέες συνθήκες έτσι ώστε ένα ή περισσότερα λογικά χαρακτηριστικά γίνονται αντιληπτά για να αφομοιωθούν από το σύστημα. Για να έχουν έξυπνη συμπεριφορά, τα CI συστήματα σχεδιάζονται συχνά έτσι ώστε να μοντελοποιούν όψεις βιολογικής και φυσικής νοημοσύνης.

Συνεπώς τα συστήματα Υπολογιστικής Νοημοσύνης είναι συνήθως υβρίδια των συστημάτων : Εξελεκτικού Υπολογισμού (Evolutionary Computation -EC), Τεχνητών Νευρωνικών Δικτύων (Artificial Neural Networks-ANN) και τα Ασαφή Συστήματα (Fuzzy Systems-FZ).

Σε αυτό το κεφάλαιο θα παρουσιαστούν αυτές οι μέθοδοι, έτσι ώστε στη συνέχεια να αναλυθεί η χρήση τους στην κρυπτανάλυση.

3.1 Evolutionary Computation (Εξελικτικός Υπολογισμός)

Ο Evolutionary Computation – EC (Εξελεγκτικός Υπολογισμός) είναι ένας κλάδος της τεχνητής νοημοσύνης που εμπνέεται από εξελικτικούς μηχανισμούς όπως η φυσική επιλογή και η προσαρμοστική συμπεριφορά για να σχεδιαστούν μέθοδοι βελτιστοποίησης και ταξινόμησης. Η φυσική επιλογή αφορά στην επιβίωση των καταλληλότερων μέσω της αναπαραγωγής. Ένας απόγονος πρέπει να διατηρήσει εκείνα τα χαρακτηριστικά των γονιών του που είναι καταλληλότερα για να επιβιώσει σε ένα συγκεκριμένο περιβάλλον. Οι αδύναμοι απόγονοι θα χάσουν τη μάχη της επιβίωσης. Τα παραδείγματα του EC που σχηματίζουν αυτή τη κατηγορία είναι:

- Γενετικοί Αλγόριθμοι (Genetic Algorithms- GA)
- Γενετικός Προγραμματισμός (Genetic Programming - GP)
- Εξελεγκτικός Προγραμματισμός (Evolutionary Programming - EP)
- Εξελεγκτικές Στρατηγικές (Evolution Strategies - ES)
- Διαφορική Εξέλιξη (Differential Evolution -DE)

Η κοινωνική και προσαρμοστική συμπεριφορά των ζώων που είναι οργανωμένα σε ομάδες ενέπνευσαν την ανάπτυξη νέας κατηγορίες EC μεθόδων , με όνομα Swarm Intelligence (SI)- Νοημοσύνη Σμήνους .Αυτές οι μέθοδοι μοντελοποιούν τις κοινωνικές διαδικασίες των ζωντανών οργανισμών που ζουν σε ομάδες και δρουν για ένα συγκεκριμένο σκοπό. Τυπικά παραδείγματα είναι οι μηχανισμοί αναζήτησης τροφής για κοπάδια ψαριών, σμήνη πουλιών και αποικίας μυρμηγκιών. Η μελέτη πολλών βιολογικών διαδικασιών κοινωνικής και προσαρμοστικής συμπεριφοράς οδήγησαν στην γνώμη ότι το να μοιράζονται πληροφορίες τα μέλη μιας ομάδας μπορεί να παράγει εξελεγκτικό πλεονέκτημα.

Τέτοιες μέθοδοι ΕC είναι :

- Particle Swarm Optimization (PSO)- Βελτιστοποίηση Σμήνους Σωματιδίων
- Ant Colony Optimization (ACO)- Βελτιστοποίηση Αποικίας Μυρμηγκιών

3.1.1 Γενετικοί Αλγόριθμοι

Τα πειράματα των βιολόγων στην προσομοίωση φυσικών γενετικών συστημάτων χρησιμοποιώντας υπολογιστές, οδήγησε στους Γενετικούς Αλγορίθμους (Genetic Algorithms -GA). Ο John Holland έχει αναγνωριστεί ως ο δημιουργός του τομέα των Gas. Μελέτησε την μηχανική νοημοσύνη και την μηχανική εκμάθηση και ανέπτυξε τις ικανότητες των Gas στα συστήματα τεχνητής νοημοσύνης. Αυτά τα συστήματα είχαν την ικανότητα να προσαρμόζονται στις αλλαγές του περιβάλλοντος και επέδειξαν επίσης αυτό-προσαρμοστικότητα υπό την έννοια ότι μπορούσαν να προσαρμόσουν τις λειτουργίες τους σύμφωνα με την αλληλεπίδραση τους με το περιβάλλον. Μέσα στις καινοτομίες του Holland ήταν η χρήση του πληθυσμού ατόμων για την διαδικασία έρευνας, αντί για ένα μόνο σημείο έρευνας.

Οι βασικές έννοιες των Gas είναι η φυσική εξέλιξη και η γενετική κληρονομικότητα. Στην φυσική εξέλιξη κάθε βιολογικό είδος πρέπει να ψάξει για την καταλληλότερη προσαρμογή σε ένα περίπλοκο και μεταβαλλόμενο περιβάλλον για να διασφαλίσει την επιβίωση του. Οι Gas βασίζονται στην ιδέα ότι η γνώση και η εμπειρία που κερδίζει ένα είδος περνάει στα χρωμοσώματα των μελών του. Για αυτό το λόγο το λεξιλόγιο που χρησιμοποιείται για τους Gas είναι αυτό της γενετικής. Κάθε μέλος του πληθυσμού ονομάζεται χρωμόσωμα (chromosomes) ή γονότυπος (genotypes). Κάθε χρωμόσωμα αποτελείται από κομμάτια που λέγονται γονίδια (genes) και κάθε ένα από αυτά είναι υπεύθυνα για την κληρονομιά ενός ή περισσότερων χαρακτηριστικών. Η εξελεγκτική διαδικασία ενός πληθυσμού χρωμοσωμάτων ανταποκρίνεται στην έρευνα ενός χώρου με πολλές πιθανές λύσεις και πρέπει να ισορροπήσει μεταξύ δύο πεδίων, την εκμετάλλευση των καλύτερων λύσεων και την εξερεύνηση του χώρου έρευνας. Η διαδικασία εξέλιξης των Gas πραγματοποιείται με δύο λειτουργίες , την διασταύρωση (crossover) και τη μετάλλαξη (mutation). Αυτές οι λειτουργίες αλλάζουν χρωμοσώματα για να παραχθούν καλύτερα. Η επιλογή του νέου πληθυσμού ολοκληρώνεται χρησιμοποιώντας ως κριτήριο ένα μέτρο καταλληλότητας. Όσο αφορά στην παρουσίαση των χρωμοσωμάτων, οι Gas συνήθως χρησιμοποιούν δυαδική αναπαράσταση, αλλά έχουν αναπτυχθεί και μέθοδοι που χρησιμοποιούν άλλα αριθμητικά συστήματα, όπως οι αριθμοί κινητής υποδιαστολής. Οι Γενετικοί Αλγόριθμοι έχουν επιτυχώς εφαρμοστεί σε προβλήματα βελτιστοποίησης διαφορετικών πεδίων, όπως το πρόβλημα του πλανόδιου πωλητή, οικονομικών κ.α.

3.1.2 Εξελικτικός Προγραμματισμός (Evolutionary Programming -EP)

Ο τομέας αυτός αναπτύχθηκε παράλληλα με αυτόν των Gas , από τον Larry Fogel. Ο σκοπός του ΕΡ ήταν η εξέλιξη της τεχνητής νοημοσύνης προβλέποντας τις αλλαγές του περιβάλλοντος. Το περιβάλλον στο ΕΡ περιγράφεται ως μία ακολουθία συμβόλων από ένα ορισμένο σύνολο και οι αλγόριθμοι της εξέλιξης δίνουν ως εκροή ένα νέο σύμβολο. Τ σύμβολο πρέπει να μεγιστοποιήσει την κατάλληλη συνάρτηση που χρησιμοποιείται ως μέτρο για την ακρίβεια της πρόβλεψης. Για την αναπαράσταση από κάθε ένα άτομο του πληθυσμού επιλέχθηκαν μηχανές πεπερασμένης κατάστασης. Ο ΕΡ , χρησιμοποιεί την αρχή της επιλογής του καταλληλότερου για τον νέο πληθυσμό, αλλά μόνο οι μηχανισμοί μετάλλαξης χρησιμοποιούνται για να αλλάξουν τα άτομα του πληθυσμού. Σε αυτή την αρχική μορφή ΕΡ, προστίθενται άλλες δύο βασικές έννοιες. Η πρώτη αφορά την ικανότητα χειρισμού συνεχόμενων παραμέτρων μαζί με

τις διακριτές και η δεύτερη η ικανότητα αυτοπροσαρμογής. Με αυτά τα νέα προνόμια, ο EP μπορεί να ανταπεξέλθει σε προβλήματα βελτιστοποίησης και ταξινόμησης με εφαρμογή σε διάφορα επιστημονικά πεδία, όπως τα οικονομικά.

3.1.3 Στρατηγικές Εξέλιξης (Evolution Strategies -ES)

Την δεκαετία του ’70, οι Ingo Rechenberg και Hans –Paul Schwefel χρησιμοποίησαν την ιδέα της μετάλλαξης προσπαθώντας να πετύχουν το βέλτιστο σχέδιο για μία σειρά συνδέσμων σε ένα σωλήνα μεταφοράς υγρών. Οι κλασσικές τεχνικές βελτιστοποίησης που χρησιμοποιούν την βαθμίδα της λειτουργίας φυσικής κατάστασης δεν ήταν ικανές να χειριστούν το πρόβλημα και η μόνη λύση ήταν να πειραματιστούν με την μετάλλαξη. Η χρήση της μετάλλαξης προκάλεσε μια μικρή διατάραξη στις καλύτερες υπάρχουσες λύσεις των προβλημάτων με στόχο να εξερευνηθεί στοχαστικά τα σημεία του ερευνητικού χώρου του προβλήματος. Το πείραμα αυτό ήταν η αρχή της ανάπτυξης των ES, που καθιερώθηκαν το 1973. Οι ES μπορούν να θεωρηθούν σαν εξελεγκτικά προγράμματα που χρησιμοποιούν αναπαράσταση κυμαινόμενου σημείου και έναν ανασχεδιασμό και ένα μηχανισμό μετάλλαξης. Χρησιμοποιούνται για την λύση διάφορων προβλημάτων βελτιστοποίησης με συνεχώς εναλλασσόμενες παραμέτρους και έχουν πρόσφατα αναπτυχθεί για διακεκριμένα προβλήματα.

3.1.4 Γενετικός Προγραμματισμός (Genetic Programming- GP)

Ο Γενετικός Προγραμματισμός αναπτύχθηκε πρόσφατα από τον Koza. Η ιδέα πίσω από τον GP είναι η εξής : αντί της κατασκευής ενός εξελεγκτικού προγράμματος για να λυθεί το πρόβλημα, να εντοπιστεί στον χώρο των μηχανικών προβλημάτων το πιο κατάλληλο για την συγκεκριμένη περίπτωση. Ο GP δίνει τα μέσα για να επιτευχθεί αυτός ο στόχος. Ένα πλήθος εκτελέσιμων προγραμμάτων δημιουργείται και κάθε ατομικό πρόγραμμα ανταγωνίζεται με τα υπόλοιπα. Τα μη επαρκή προγράμματα αδρανούν ενώ τα καλύτερα αναπαράγονται με μέσα μηχανισμών όπως η διασταύρωση και η μετάλλαξη. Η αξιολόγηση των προγραμμάτων τελειώνει χρησιμοποιώντας ένα κατάλληλο σε ένα προκαθορισμένο σετ προβλημάτων.

3.1.5 Διαφορική Εξέλιξη (Differential Evolution-DE)

Η Διαφορική Εξέλιξη , DE, είναι μία αριθμητική παράλληλη άμεση μέθοδος έρευνας, που χρησιμοποιεί N,D-διαστάσεων παραμετρικά διανύσματα $x_{i,G}$, i=1,2,..,N, σαν πληθυσμός για κάθε επανάληψη (γενιά) του αλγόριθμου. Σε κάθε γενιά, οι διαδικασίες μετάλλαξης και διασταύρωσης εφαρμόζονται στα άτομα, για να παραχθεί νέος πληθυσμός , ο οποίος ακολούθως υποβάλλεται σε φάση επιλογής.

Για κάθε παράγοντα $x_{i,G,}$ i= 1,2,…,N ένας μεταλλαγμένος παράγοντας δημιουργείται μέσα από την ακόλουθη συνάρτηση :

$u_{i,G+1} = x_{r1,G} + F(x_{r2,G} – x_{r3,G})$ (1.5)

όπου r_1, r_2,r_3 ∈ (1,2,..N , είναι τυχαίοι αριθμητικοί δείκτες, αμοιβαία διαφορετικοί και διαφορετικοί από το i και F∈(0,2) . Ακολουθεί η φάση της μετάλλαξης, όπου η διασταύρωση εφαρμόζεται στο μεταλλαγμένο διάνυσμα και παράγεται το διάνυσμα δοκιμής, $u_{i, G+1}$ = ($u_{1i,G+1,}$ $u_{2i,G+1}$,…., $u_{Di,G+1}$) , όπου

$$u_{ji,G+1} = \begin{cases} v_{ji,G+1}, & \text{if } (\text{randb}(j) \leqslant CR) \text{ or } j = \text{rnbr}(i), \\ x_{ji,G}, & \text{if } (\text{randb}(j) > CR) \text{ and } j \neq \text{rnbr}(i) \end{cases} \quad (1.6)$$

για j =1,2,…,D όπου randb(j) είναι η $j^{η}$ αξιολόγηση μιας ομοιόμορφης τυχαίας γεννήτριας αριθμών στο πεδίο [0,1], CR είναι η σταθερά της διασταύρωσης στο εύρος [0,1] και rnbr(i) είναι ένα τυχαία

επιλεγμένο περιεχόμενο του συνόλου {1,2,…,D} .Για να αποφασιστεί αν το διάνυσμα $u_{i,G+1}$ θα είναι μέλος του πληθυσμού της επόμενης γενιάς, συγκρίνεται με το αρχικό διάνυσμα $x_{i,G.}$

Επομένως,

$$x_{i,G+1} = \begin{cases} u_{i,G+1}, & \text{if } f(u_{i,G+1}) < f(x_{i,G}), \\ x_{i,G}, & \text{otherwise.} \end{cases}$$

Ο DE αλγόριθμος που χρησιμοποιεί τον μηχανισμό μετάλλαξης της (1.5) λέγεται σταθερή μεταβλητή του DE αλγόριθμου. Διαφορετικοί μηχανισμοί μετάλλαξης ορίζουν τις άλλες μεταβλητές του DE αλγορίθμου. Οι μηχανισμοί μετάλλαξης που έχουν εφαρμοστεί με υποσχόμενα αποτελέσματα είναι οι εξής :

$$v_{i,G+1} = x_{\text{best},G} + F(x_{r_1,G} - x_{r_2,G}), \tag{1.8}$$

$$v_{i,G+1} = x_{i,G} + F(x_{\text{best},G} - x_{i,G}) + F(x_{r_1,G} - x_{r_2,G}), \tag{1.9}$$

$$v_{i,G+1} = x_{\text{best},G} + F(x_{r_1,G} + x_{r_2,G} - x_{r_3,G} - x_{r_4,G}), \tag{1.10}$$

$$v_{i,G+1} = x_{r_1,G} + F(x_{r_2,G} + x_{r_3,G} - x_{r_4,G} - x_{r_5,G}), \tag{1.11}$$

Όπου $x_{best,G}$ ανταποκρίνεται στη καλύτερη επιλογή της G^{th} γενιάς, r_1 ,r_2, r_3,r_4,$r_5 \in$ {1,2,..,N}, είναι αμοιβαία διαφορετικοί αριθμητικοί δείκτες και $x_{i,G}$ είναι το τρέχον άτομο της γενιάς G.

3.1.6 Βελτιστοποίηση Αποικίας Μυρμηγκιών (Ant Colony Optimization-ACO)

Ο ACO αλγόριθμος είναι μία μέθοδος Σμήνους Ευφυίας για την επίλυση συνδυαστικών προβλημάτων βελτιστοποίησης γενικά, όπως το πρόβλημα του πλανόδιου πωλητή και του σχεδιασμού τηλεπικοινωνιών. Χρησιμοποιεί έναν πληθυσμό μελών που ονομάζονται τεχνητά μυρμήγκια και εμπνεύστηκε από πειράματα με αποικίες με αληθινά μυρμήγκια. Σε αυτά τα πειράματα ανακαλύφθηκε ότι μετά από λίγο χρόνο, κάποια μυρμήγκια βρίσκαν τον συντομότερο δρόμο για να μεταφέρουν την τροφή τους. Αυτή η ικανότητα γίνεται δυνατή χάρη σε μία χημική ουσία την φερομόνη, την οποία τα μυρμήγκια αφήνουν στο περιβάλλον, εξυπηρετώντας έναν έμμεσο μηχανισμό επικοινωνίας. Στην αρχή, η επιλογή της διαδρομής γίνεται τυχαία, αλλά καθώς περνάει η ώρα, η πιθανότητα να επιλεγεί το συντομότερο μονοπάτι γίνεται υψηλότερη και η ποσότητα της φερομόνης σε αυτό το μονοπάτι αυξάνεται γρηγορότερα συγκρινόμενη με αυτή στα μονοπάτια με μεγαλύτερο μήκος. Αυτή η απλή ιδέα προσομοιώθηκε από τις μεθόδους ACO για να εντοπίζει λύσεις και να ανταποκρίνεται σε δύσκολα προβλήματα βελτιστοποίησης.

3.1.7 Βελτιστοποίηση Σμήνους Σωματιδίων- Particle Swarm Optimization (PSO)

Η μέθοδος αυτή, έχει γίνει δημοφιλής τα τελευταία 15 χρόνια. Η αποτελεσματικότητα και η αποδοτικότητα της την έχει αναδείξει σε μια πολύτιμη προσέγγιση σε διάφορα επιστημονικά πεδία όπου υπάρχουν περίπλοκα προβλήματα βελτιστοποίησης. Επίσης έχει εύκολη εφαρμογή. Είναι ένας αλγόριθμος που ο βασικός ερευνητικός μηχανισμός του βασίζεται σε μια ομάδα/πληθυσμό *ερευνητικών παραγόντων* που επαναληπτικά αλλάζουν την θέση τους σε έναν ερευνητικό χώρο Χ. Ο πληθυσμός ονομάζεται σμήνος (swarm) και τα άτομα σωματίδια (particles). Κάθε σωματίδιο κινείται με συγκεκριμένη ταχύτητα στον χώρο έρευνας και διατηρεί στην μνήμη του την καλύτερη θέση που μετρήθηκε. Η γειτονιά ενός σωματιδίου είναι το δίκτυο ανταλλαγής πληροφοριών του σωματιδίου με ένα υποσύνολο του σμήνους.

Όταν κάθε σωματίδιο συνδέεται με όλα τα άλλα και η γειτονιά των σωματιδίων παραμένει αμετάβλητη στις αλλαγές ενώ τρέχει ο αλγόριθμος, τότε έχουμε την *global* (παγκόσμια) εκδοχή της PSO. Σε αυτή την περίπτωση, η καλύτερη θέση που ανακτήθηκε από όλα τα σωματίδια του σμήνους ανακοινώνεται σε όλα τα μέλη.

Όταν τα σωματίδια είναι συνδεδεμένα αραιά και οι γειτονιές είναι υποσύνολα του συνολικά πληθυσμού, έχουμε την *local* (τοπική) εκδοχή της PSO,όπου σε κάθε σωματίδιο ανατίθεται μία γειτονιά που αποτελείται από ένα προκαθορισμένο αριθμό σωματιδίων. Σε αυτή τη περίπτωση, η καλύτερη θέση που ανακτήθηκε από τα σωματίδια που αποτελούν την γειτονιά κοινοποιείται μεταξύ τους.

Έστω ένας D- διαστάσεων ερευνητικός χώρος, $S \subset \mathbb{R}^D$ και ένα σμήνος N σωματιδίων. Το i*th* σωματίδιο είναι ένα D- διαστάσεων διάνυσμα $X_i = (x_{i1}, x_{i2}, x_{i\,D})^T$. Η ταχύτητα του σωματιδίου είναι επίσης ένα D- διαστάσεων διάνυσμα $V_i = (v_{i1},v_{i2,..},v_{i\,D})^T$.Η καλύτερη προηγούμενη θέση που μετρήθηκε ποτέ από το i-th σωματίδιο είναι ένα σημείο στο S , καθορισμένο από $P_i =(p_{i1},p_{i2},...,p_{i\,D})^T$. Έστω g, ο αριθμητικός δείκτης του σωματιδίου που ανέκτησε την καλύτερη προηγούμενη θέση ανάμεσα σε όλα τα άτομα του σμήνους (global PSO) ή ανάμεσα στα άτομα της γειτονιάς του i-th σωματιδίου (local PSO).

Έπειτα, σύμφωνα με τον έκδοση του συντελεστή συστολής του PSO το σμήνος λειτουργεί χρησιμοποιώντας αυτές τις εξισώσεις :s

$$V_i^{(t+1)} = \chi \left(V_i^{(t)} + c_1 r_1 \left(P_i^{(t)} - X_i^{(t)} \right) + c_2 r_2 \left(P_g^{(t)} - X_i^{(t)} \right) \right),$$
$$X_i^{(t+1)} = X_i^{(t)} + V_i^{(t+1)},$$

Όπου i= 1,2,..,N είναι ο συντελεστής συστολής, c1 και c2 ορίζουν την γνωστική και κοινωνική παράμετρο , r_1, r_2 είναι τυχαίοι αριθμοί ομοιόμορφα κατανεμημένοι στο εύρος [0,1] και t είναι ο μετρητής των επαναλήψεων. Η αξία του συντελεστή συστολής διαμορφώνεται σύμφωνα με τον τύπο:

$\chi = 2\kappa / |2 - \varphi - \sqrt{\varphi^2 - 4\varphi}|$, με ϕ= c_1+ c_2 και k=1.

Οι προκαθορισμένες αξίες της παραμέτρου ,σύμφωνα με την βιβλιογραφία, είναι x= 0.729 και c_1=c_2 = 2.05.

Σε μία διαφορετική εκδοχή της PSO χρησιμοποιείται μία παράμετρος που λέγεται βάρος αδράνειας, *inertia weight* και το σμήνος διαμορφώνεται σύμφωνα με τον τύπο :

$$V_i^{(t+1)} = w V_i^{(t)} + c_1 r_1 \left(P_i^{(t)} - X_i^{(t)} \right) + c_2 r_2 \left(P_g^{(t)} - X_i^{(t)} \right),$$
$$X_i^{(t+1)} = X_i^{(t)} + V_i^{(t+1)},$$

Όπου i= 1,2,…,,N και w είναι το βάρος αδράνειας ,ενώ όλες οι άλλες μεταβλητές είναι ίδιες με την εκδοχή του συντελεστή συστολής. Δεν υπάρχει συγκεκριμένος τύπος για τον ορισμό του παράγοντα w, που ελέγχει την επίπτωση της προηγούμενης ιστορίας των ταχυτήτων στην τρέχουσα. Ωστόσο, ένα μεγάλο βάρος αδράνειας διευκολύνει καθολική (global) εξερεύνηση (έρευνα νέων περιοχών), ενώ ένα μικρό τείνει να διευκολύνει τοπική εξερεύνηση (local) (καλύτερη έρευνα της τρέχουσας περιοχής έρευνας), ενστικτωδώς φαίνεται προτιμότερο η ρύθμιση σε μεγάλη αξία και η σταδιακή μείωση για την απόκτηση καταλληλότερων λύσεων. Αυτή η προσέγγιση έχει πιστοποιηθεί πειραματικά. Μία αρχική αξία περίπου 1.2 και η βαθμιαία μείωση προς 0.1 θεωρείται μία καλή επιλογή για το w. Η κατάλληλη ρύθμιση των c1,c2 οδηγεί σε γρηγορότερη σύγκλιση των τοπικών ελάχιστων. Ως προκαθορισμένες τιμές έχουν προταθεί c1=c2=2 , αλλά τα αποτελέσματα πειραμάτων δείχνουν ότι εναλλακτικές διαμορφώσεις, ανάλογα το πρόβλημα, μπορούν να παράξουν καλύτερα αποτελέσματα.

Για να αποφευχθεί η ύπαρξη ταχυτήτων με υψηλές τιμές που θα οδηγήσει σε διακυμάνσεις των σωματιδίων εκτός της περιοχής έρευνας και συνεπώς καταστροφής της

μεθόδου, ορίζεται μία μέγιστη τιμή για την ταχύτητα η Vmax, για κάθε συντεταγμένη της ταχύτητας. Τυπικά το σμήνος και οι ταχύτητες αρχικοποιούνται τυχαία στον χώρο αναζήτησης.

3.2 Τεχνητά Νευρωνικά Δίκτυα (Artificial Neural Networks- ANN)

Η πολυπλοκότητα και οι παράλληλες λειτουργίες που μπορεί να εκτελεί το ανθρώπινο μυαλό ενέπνευσαν τον σχεδιασμό των Τεχνητών Νευρωνικών Δικτύων, TNN, (Artificial Neural Networks -ANN). Ένα TNN είναι ένα δίκτυο που αποτελείται από διάφορα εσωτερικά επίπεδα που λέγονται *hidden layers* ,κρυμμένα επίπεδα, τα οποία ποικίλλουν στον αριθμό και τον αριθμό των εσωτερικών τους κόμβων, τους νευρώνες, *neurons.* Το πρώτο επίπεδο, το στρώμα εισροής,*input layer,* όπου εισέρχονται τα δεδομένα. Αυτό ενώνεται με το δεύτερο και ούτω καθεξής ως το *output layer,* στρώμα εκροής που παράγει την πρόβλεψη του μοντέλου. Είναι ένας μαζικά παράλληλα κατανεμημένος επεξεργαστής, αποτελούμενος από απλές μονάδες (neurons) χαρακτηρίζονται από μία έμφυτη ικανότητα να αποκτούν γνώση από δεδομένα μέσα μία διαδικασία εκμάθησης. Η γνώση αποθηκεύεται σε συνδέσμους εσωτερικά των νευρώνων, τα βάρη (weights), κάνοντας τη διαθέσιμη για χρήση. Κάθε τεχνητός νευρώνας εκτελεί ένα τοπικό υπολογισμό.

Η εκροή του υπολογισμού αυτού καθορίζεται από την εισροή του νευρώνα και την συνάρτηση ενεργοποίησης του. Η όλη λειτουργικότητα του δικτύου καθορίζεται από την τοπολογία (αρχιτεκτονική) του, τον αριθμό των νευρώνων και το μοτίβο διασύνδεσης του, τον αλγόριθμο που εκτελεί και τα χαρακτηριστικά των νευρώνων.

Τα TNN μπορούν να κατηγοριοποιηθούν βάση της τοπολογίας τους, της λειτουργικότητας τους, των μεθόδων τους και άλλων χαρακτηριστικών. Όσο αφορά στην αρχιτεκτονική τους, τα πιο απλά νευρωνικά δίκτυα έχουν ένα μόνο επίπεδο νευρώνων και ονομάζονται single-layer TNN (μοναδικού επιπέδου) , ενώ αυτά με περισσότερα επίπεδα λέγονται multi-layer (πολλαπλών επιπέδων) TNN. Τα TNN με απεριοδικές συνδέσεις εντός των νευρώνων ονομάζονται Feedforward Neural Networks (FNNs) (Νευρωνικά Δίκτυα πρόσθιας Τροφοδότησης)και αυτά με βρόχους ανατροφοδότησης λέγονται Reccurent Neural Networks (RNNs) (Επαναλαμβανόμενα Νευρωνικά Δίκτυα). Τα πιο συχνά χρησιμοποιούμενα TNNs είναι τα FNNs. Ένα τέτοιο νευρωνικό δίκτυο είναι ένα δίκτυο με απεριοδικές και μονής κατεύθυνσης άμεσες συνδέσεις εντός των νευρώνων, όπου οι νευρώνες μπορούν να ταξινομηθούν σε στρώματα. Έτσι, η τοπολογία του δικτύου μπορεί να οριστεί ως μία σειρά ακεραίων όπου ο καθένας αντιπροσωπεύει τον αριθμό των μονάδων που ανήκουν στο συγκεκριμένο στρώμα.

Κάθε νευρώνας έχει ένα σύνολο εισερχόμενων τιμών z_1, z_2,.. οι οποίες είναι πραγματικοί αριθμοί μεταξύ 0 και 1 και έχει ένα σύνολο βαρών w_1, w_2 ,… σχετισμένα με κάθε εισροή και ένα συνολικό bias b. Τα βάρη ορίζονται τυχαία και ο αλγόριθμος αλλάζει κατά τη διάρκεια της εκτέλεσης.

Η λειτουργικότητα των TNNs βασίζεται στον τύπο των νευρώνων από τους οποίους αποτελούνται και τη συνάρτηση ενεργοποίησης τους. Γενικά υπάρχουν δύο τύποι νευρώνων, οι αθροιστές (*summing)* και οι παραγωγικοί *product* νευρώνες. Οι πρώτοι εφαρμόζουν την συνάρτηση ενεργοποίησης στο σύνολο των εισερχόμενων βαρών ,ενώ οι παραγωγικοί στην εκροή των εισροών των βαρών. Η συνάρτηση ενεργοποίησης καθορίζει την εκροή του νευρώνα και πολλά είδη συναρτήσεων ενεργοποίησης μπορούν να χρησιμοποιηθούν.

Οι πιο συχνά χρησιμοποιούμενες είναι η γραμμική, η συνάρτηση κατωφλίου, η σιγμοειδής, η συνάρτηση υπερβολής και η συνάρτηση Gaussian. Με αυτή τη σειρά, είναι οι εξής:

$$f_1(x) = \alpha x,$$

$$f_2(x) = \begin{cases} \alpha_1, & \text{if } x \geqslant \theta, \\ \alpha_2, & \text{if } x < \theta, \end{cases}$$

$$f_3(x) = \frac{1}{1 + e^{-\lambda_1 x}},$$

$$f_4(x) = \tanh(\lambda_2 x),$$

$$f_5(x) = e^{-x^2/\sigma^2},$$

Όπου α,α_1 ,α_2 ,θ, λ_1 ,λ_2 είναι σταθερές και σ^2 είναι η διακύμανση στη Γκαουσιανής συνάρτησης.

Οι μέθοδοι των Τεχνητών Νευρωνικών Δικτύων (ΤΝΝ)χωρίζονται σε τρείς κατηγορίες, ανάλογα με την μάθηση. Μάθηση (learning/training) είναι η διαδικασία της τροποποίησης της τιμής των βαρών του δικτύου, ώστε δοθέντος συγκεκριμένου διανύσματος εισόδου να παραχθεί συγκεκριμένο διάνυσμα εξόδου.

- Μάθηση υπό επίβλεψη (supervised learning), όπου τα ΤΝΝ πρέπει να προσαρμοστούν στα δοθέντα δεδομένα για την παραγωγή συγκεκριμένης εκροής
- Μάθηση χωρίς επίβλεψη (unsupervised learning), όπου τα ΤΝΝ πρέπει να βρουν πρότυπα στα εισερχόμενα δεδομένα.
- Ενισχυτική μάθηση (reinforcement learning) , που στόχο έχει την επιβράβευση των ΤΝΝ σε περίπτωση καλής λειτουργίας και σε τιμωρία στην αντίθετη περίπτωση.

Στην περίπτωση της μάθησης υπό επίβλεψη, στόχος είναι να δοθούν στα βάρη ,W, τιμές τέτοιες ώστε η διαφορά μεταξύ της επιθυμητής εκροής και της πραγματικής να ελαχιστοποιηθεί. Η διαδικασία ξεκινά με την παρουσίαση στο δίκτυο μίας σειράς προτύπων για τα οποία οι επιθυμητές εκροές είναι γνωστές εκ των προτέρων και υπολογίζεται μία συνάρτηση συνολικού λάθους

$$E = \sum_{k=1}^{P} \bar{E}_k.$$

P είναι ο αριθμός των προτύπων και E_K είναι το μερικό λάθος δικτύου σύμφωνα με το k_{th} πρότυπο. Διάφορες συναρτήσεις χρησιμοποιούνται για τον υπολογισμό του λάθους. Συνήθως υπολογίζεται από το άθροισμα της τετραγωνικής διαφοράς μεταξύ των πραγματικών και των επιθυμητών εκροών του προτύπου. Τα πρότυπα εκμάθησης μπορούν να παρουσιαστούν πολλές φορές στο δίκτυο. Κάθε πέρασμα όλων των προτύπων που ανήκουν στο σετ εκμάθησης , Τ, λέγεται μία εποχή (training epoch). Το σύνολο των απαιτούμενων εποχών θωρείται η ταχύτητα του αλγορίθμου εκπαίδευσης.

Η υπολογιστική δύναμη των νευρωνικών δικτύων αντλείται από την παράλληλη και διανεμημένη δομή και την έμφυτη ικανότητα τους να προσαρμόζονται σε συγκεκριμένα προβλήματα, να μαθαίνουν και να γενικεύουν. Αυτά τα χαρακτηριστικά επιτρέπουν στα ΤΝΝ να λύνουν περίπλοκα προβλήματα. Έχουν χρησιμοποιηθεί σε πολλά επιστημονικά πεδία με δύσκολα και πολύπλοκα προβλήματα. Τέτοιο πεδίο φυσικά είναι η κρυπτογραφία και στη περίπτωση που μας αφορά, η κρυπτανάλυση.

3.3 Ασαφή Συστήματα. (Fuzzy Systems)

Η θεωρία συνόλων και η δυαδική λογική απαιτούν δύο αξίες παραμέτρων, το να είναι μέρος του συνόλου ή όχι , και 0 ή 1,αντίστοιχα. Η ανθρώπινη συλλογιστική ωστόσο, περιλαμβάνει ένα μέτρο αμφιβολίας και για αυτό δεν είναι ακριβές. Με τα ασαφή σύνολα και την ασαφή λογική επιτρέπεται ο κατά προσέγγιση συλλογισμός. Στα ασαφή σύνολα, ένα στοιχείο ανήκει σε ένα σύνολο με συγκεκριμένο βαθμό βεβαιότητας. Η ασαφής λογική, επιτρέπει αιτιολόγηση σε αυτά τα αβέβαια γεγονότα να συμπεραίνουν νέα γεγονότα με ένα βαθμό βεβαιότητας συσχετισμένο με κάθε γεγονός. Κατά μία έννοια, τα ασαφή συστήματα επιτρέπουν την μοντελοποίηση της κοινής λογικής. Η αβεβαιότητα των ασαφών συστημάτων αναφέρεται ως μη στατιστική αβεβαιότητα, η οποία δεν θα πρέπει να συγχέεται με τη στατιστική αβεβαιότητα. Η στατιστική αβεβαιότητα βασίζεται στους νόμους των πιθανοτήτων, ενώ η μη στατιστική αβεβαιότητα στηρίζεται στην ασάφεια και στην ανακρίβεια. Η στατιστική αβεβαιότητα λύνεται με την παρατήρηση. Η μη στατιστική αβεβαιότητα, ή ασάφεια, είναι μία έμφυτη ιδιότητα ενός συστήματος και δεν μπορεί να αλλάξει ή να διερευνηθεί μέσω της παρατήρησης.

ΚΕΦΑΛΑΙΟ 4ο : ΚΡΥΠΤΑΝΑΛΥΣΗ ΜΕ ΤΙΣ ΜΕΘΟΔΟΥΣ PSO ΚΑΙ DIFFERENTIAL EVOLUTION

Ο τομέας της κρυπτανάλυσης είναι απαιτητικός και περίπλοκος. Συνεπώς, η εφαρμογή ενός τόσο αποδοτικού και αποτελεσματικού εργαλείου όπως η Τεχνητή Νοημοσύνη στον τομέα, είναι φυσικό επακόλουθο. Μία σύντομη επισκόπηση σχετικών ερευνών ακολουθεί :

- 1979 Relaxation Algorithms: Η δουλειά των Peleg and Rosenfeld το 1979, των Hunter and McKenzie το 1983, των Carrol and Martin το 1986, και των King and Bahler το 1992 που χρησιμοποιούσαν *αλγόριθμους χαλάρωσης* για να σπάνε απλά κρυπτογραφήματα θεωρούνται οι προκάτοχοι της εφαρμογής των μεθόδων εξελικτικού υπολογισμού στην κρυπτανάλυση.
- 1993 Genetic Algorithms – Simulated Annealing method : Το 1993 Spillman et. Al. εισήγαγαν την χρήση Γενετικών Αλγορίθμων για την επίλυση απλών κρυπτογραφημάτων μεταφοράς και το πρόβλημα σακιδίου. Τον ίδιο χρόνο οι Forsyth and Safavi-Naini πρότειναν την μέθοδο προσομοίωσης ανόπτησης για επίλυση απλών κρυπτογραφημάτων.
- 1996, Genetic Algorithms : Οι Vertan and Geangala χρησιμοποίησαν Γενετικούς Αλγόριθμους για να λύσουν το κρυπτογράφημα Merkle- Hellman. (κρυπτογράφημα δημοσίου κλειδιού, ειδική περίπτωση προβλήματος σακιδίου)
- 1997, Genetic Algorithms : Bagnall et al. παρουσίασαν μία Ciphertext-only επίθεση χρησιμοποιώντας Γενετικούς Αλγόριθμους για την επίθεση σε απλοποιημένη έκδοση ρότορα Enigma.
- 1998: Ο A.Clark πρότεινε τον αλγόριθμο αναζήτησης tabu για κρυπτανάλυση και συνέκρινε πολλές ευρετικές τεχνικές, όπως και γενετικούς αλγόριθμους για την κρυπτανάλυση κλασσικών κρυπτοσυστημάτων. Οι J.Clark και Jacob παρουσίαζαν μία βελτιστοποίηση δύο σταδίων για τον σχεδιασμό συναρτήσεων Boolean και αργότερα πρότειναν νέες τεχνικές επίθεσης σε κρυπτογραφικά πρωτόγονα (κρυπτογραφικοί αλγόριθμοι χαμηλού επιπέδου) , βασισμένες σε έγχυση σφάλματος ανάλυση χρόνου. Αυτές οι μέθοδοι είναι αποτελεσματικές στην κρυπτανάλυση συγκεκριμένου είδους σχημάτων αναγνώρισης με τη χρήση προσομοίωσης ανόπτησης .
- 1998: Ο Ramzan στο Ph.D. έσπασε το Unix Crypt κρυπτοσύστημα , μία απλουστευμένη μορφή του Enigma, χρησιμοποιώντας TNN. Με τα TNN αναπτύχθηκε ένα νέο σύστημα ανταλλαγής κλειδιού, βασισμένο σε ένα νέο φαινόμενο, τα συγχρονισμένα TNN. Ωστόσο αυτό το νέο σύστημα αποδείχτηκε ότι μπορεί να κρυπταναλυθεί με τρείς διαφορετικούς τρόπους, χρησιμοποιώντας γενετικούς αλγόριθμους και πιθανολογικές επιθέσεις.
- 2002: Hernadez et.al πρότειναν μία νέα τεχνική κρυπτανάλυσης για TEA με μειωμένο αριθμό γύρων, που αποδείχτηκε να είναι αποτελεσματική στον διαχωρισμό ενός κρυπτογραφικού αλγόριθμου δέσμης από μία τυχαία παραλλαγή, εφαρμόζοντας γενετικούς αλγόριθμους.

4.1 Κρυπτανάλυση block-cipher με PSO Method.

Θα μελετηθεί η PSO ως μέθοδος κρυπτανάλυσης ενός κρυπτοσυστήματος block-cipher. Συγκεκριμένα, θα ερευνηθεί το πρόβλημα της εύρεσης bits που λείπουν από ένα κλειδί που χρησιμοποιήθηκε σε ένα απλοποιημένο κρυπτογράφημα Feistel, την DES 4 επαναλήψεων.

Η PSO θεωρεί ως πιθανή λύση έναν πραγματικό αριθμό στο εύρος [0,1]. Για την αξιολόγηση των προτεινόμενων λύσεων, η PSO στρογγυλοποιεί αξίες στον κοντινότερο ακέραιο.

Χρησιμοποιούμε global και local PSO, όλοι οι πληθυσμοί περιορίζονται στον εφικτό χώρο του προβλήματος και το μέγεθος κάθε πληθυσμού είναι 100. Η μέγιστη ταχύτητα, V_{max} ορίζεται στο 0,5. Οι παράμετροι ορίστηκαν όπως στην βιβλιογραφία, χ=0.729 και $c_1 = c_2 = 2{,}05$. Η προσέγγιση δοκιμάστηκε για διάφορα αρχικά κλειδιά και αριθμό ζευγών np. Τα αποτελέσματα για έξι διαφορετικά κλειδιά $k_i = 1,..6$ και ζεύγη δοκιμών 20,50 και 100 παρουσιάζονται αντίστοιχα στους παρακάτω πίνακες.

Table 1
Results for six different keys using $np = 20$ test pairs.

key	Method	Suc.Rate	Function Evaluations	
			mean	min
k_1	PSOCG	98%	1146	200
k_1	PSOCL	100%	2020	200
k_2	PSOCG	99%	854	200
k_2	PSOCL	100%	2079	200
k_3	PSOCG	97%	1542	200
k_3	PSOCL	100%	2300	200
k_4	PSOCG	97%	1698	200
k_4	PSOCL	100%	1884	300
k_5	PSOCG	93%	1870	200
k_5	PSOCL	100%	1788	300
k_6	PSOCG	100%	740	200
k_6	PSOCL	100%	1717	200

Table 2
Results for six different keys using $np = 50$ test pairs.

key	Method	Suc.Rate	Function Evaluations	
			mean	min
k_1	PSOCG	99%	885	200
k_1	PSOCL	100%	1873	200
k_2	PSOCG	100%	682	200
k_2	PSOCL	100%	1348	200
k_3	PSOCG	100%	606	200
k_3	PSOCL	100%	1432	200
k_4	PSOCG	96%	1322	200
k_4	PSOCL	100%	1382	200
k_5	PSOCG	98%	941	200
k_5	PSOCL	100%	1691	200
k_6	PSOCG	96%	1205	200
k_6	PSOCL	100%	1627	200

Table 3
Results for six different keys using $np = 100$ test pairs.

key	Method	Suc.Rate	Function Evaluations	
			mean	min
k_1	PSOCG	100%	640	200
k_1	PSOCL	100%	1225	200
k_2	PSOCG	97%	1082	200
k_2	PSOCL	100%	1261	200
k_3	PSOCG	99%	833	300
k_3	PSOCL	100%	1633	200
k_4	PSOCG	100%	589	200
k_4	PSOCL	100%	1255	200
k_5	PSOCG	99%	883	200
k_5	PSOCL	100%	1214	200
k_6	PSOCG	92%	2043	200
k_6	PSOCL	100%	1640	200

Παρατηρήσεις –Συμπεράσματα.

Τα πρώτα αποτελέσματα είναι ενθαρρυντικά όσον αφορά την σύγκριση με την επίθεση ωμής βίας. Με μέσο όρο τις 1500 αξιολογήσεις συνάρτησης, η μέθοδος εντοπίζει τα bits , σε σχέση με τις 2^{14} = 16384 της ωμής βίας. Βλέπουμε ότι η local PSO έχει μεγαλύτερα ποσοστά επιτυχίας. Επίσης, όσο μεγαλώνει η τιμή του np, επιταχύνεται ο ρυθμός σύγκλισης και αυξάνεται η τιμή του τοπικού ελάχιστου.

Η PSO μπορεί να επιταχύνει την μέθοδο εύρεσης των bits με επίθεση ωμής βίας, άρα μπορούμε να χρησιμοποιήσουμε τις δύο μεθόδους συνδυαστικά για καλύτερο αποτέλεσμα. Όταν παραλειφθεί η εισροή και εκροή συναρτήσεων μετάθεσης της DES , η PSO εντοπίζει 4 υποψήφιες αξίες για τα 14 bits που ψάχνουμε, που ελαχιστοποιούν την συνάρτηση αξιολόγησης, που διαφέρουν σε 2 προκαθορισμένες θέσεις που ανταποκρίνονται στις θέσεις 10 και 36 του κλειδιού DES. Καταλήγοντας, τα υποσχόμενα αποτελέσματα των πειραμάτων, δίνουν πιθανότητα ότι η PSO μέθοδος μπορεί να εντοπίσει και άλλα bits, πλην των 14 στα οποία την εφαρμόσαμε.

4.2 Η Κρυπτανάλυση ως Πρόβλημα Διακριτής Βελτιστοποίησης.

Σε αυτό το κεφάλαιο, τρία προβλήματα θα παρουσιαστούν ως προβλήματα διακριτής βελτιστοποίησης και δύο αλγόριθμοι Εξελικτικού Υπολογισμού, η μέθοδος Βελτιστοποίησης Σμήνους Σωματιδίων (PSO) και ο αλγόριθμος Διαφορικής Εξέλιξης (DE) χρησιμοποιούνται για την κρυπτανάλυση τους. Τα αποτελέσματα δείχνουν ότι η μορφοποίηση των προβλημάτων ως διακριτής βελτιστοποίησης διατηρεί την πολυπλοκότητα του, γεγονός που το καθιστά δύσκολο για τις μεθόδους να εξάγουν κομμάτια πληροφορίας. Αυτό το γεγονός καταδεικνύει ότι το κύριο πρόβλημα όταν χρησιμοποιούνται μέθοδοι Εξελικτικού Υπολογισμού είναι ο κατάλληλος ορισμός της συνάρτησης λειτουργίας, πχ η αποφυγή παραπλανητικών τοπίων που οδηγούν σε αποτελέσματα που δεν θα είναι καλύτερα από αντίστοιχα τυχαίας έρευνας. Κατόπιν αυτού, το πρώτο συμπέρασμα που εξάγεται από αυτά τα πειράματα είναι ότι λόγω της δεδομένης πολυπλοκότητας των κρυπτογραφικών προβλημάτων, όπου χρησιμοποιούνται οι μέθοδοι Εξελικτικού Υπολογισμού, πρέπει να δοθεί ιδιαίτερη προσοχή στον σχεδιασμό της συνάρτησης έτσι ώστε να περιλαμβάνει όσες περισσότερες πληροφορίες γίνεται για το πρόβλημα-στόχος. Το

δεύτερο είναι ότι οι μέθοδοι τεχνητής νοημοσύνης μπορούν να χρησιμοποιηθούν ως μία γρήγορη πρακτική μέθοδος για την αποτελεσματικότητα και αποδοτικότητα των προτεινόμενων κρυπτογραφικών συστημάτων. Τα δυνατά κρυπτογραφικά συστήματα δεν πρέπει να αποκαλύπτουν τυχόν πρότυπα των κρυπτογραφημένων μηνυμάτων τους ή την εσωτερική τους δομή, καθώς αυτό θα μπορούσε να οδηγήσει στην κρυπτανάλυση τους. Οι μέθοδοι τεχνητής νοημοσύνης μπορούν να χρησιμοποιηθούν ως ένα πρώτο μέτρο αξιολόγησης νέων κρυπτογραφικών σχημάτων, πριν άλλες πιο επίσημες μέθοδοι, πιθανώς πιο περίπλοκες, εφαρμοστούν για την ανάλυση τους.

4.2.1 1ο Πρόβλημα

Δοθέντος ενός σύνθετου ακεραίου N, βρείτε ζεύγη x, y ∈ Z_N^* , τέτοια ώστε $x^2 = y^2 \pmod N$ με

$$x \not\equiv \pm y \pmod N.$$

Το πρόβλημα ισοδυναμεί με την εύρεση μη ασήμαντων παραγόντων του N , καθώς το N χωρίζει $x^2 - y^2 = (x-y)(x+y)$, αλλά το N δεν χωρίζει ούτε x-y ή x+y . Έτσι, gcd(x-y,N) είναι μη σημαντικός παράγοντας του N.

Σχηματίζουμε το πρόβλημα ως διακριτής βελτιστοποίησης ορίζοντας τη συνάρτηση ελαχιστοποίησης

$f : \{1, 2, \ldots, N-1\} \times \{1, 2, \ldots, N-1\} \mapsto \{0, 1, \ldots, N-1\},$ με

$$f(x, y) = x^2 - y^2 \pmod N,$$

Με περιορισμούς

$$x \not\equiv \pm y \pmod N.$$

Ο περιορισμός

$$x \equiv -y \pmod N$$

Μπορεί να ενσωματωθεί στο πρόβλημα αλλάζοντας την κύρια συνάρτηση. Σε αυτή τη περίπτωση, το πρόβλημα περιορίζεται στην ελαχιστοποίηση της συνάρτησης g : { 2,3,…,(N-1)/2 x {2,3,…,(N-1)/2}→{0,1,…,N-1 }με

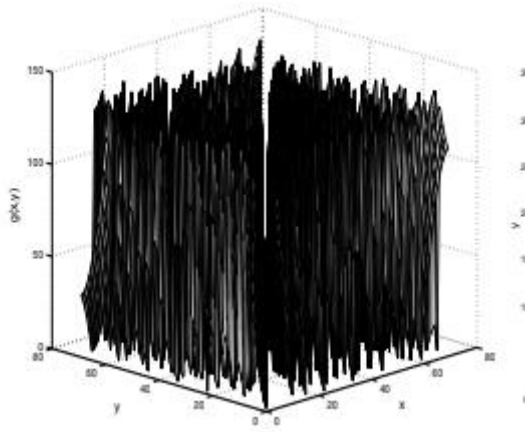
$$g(x, y) = x^2 - y^2 \pmod N,$$

Με περιορισμό

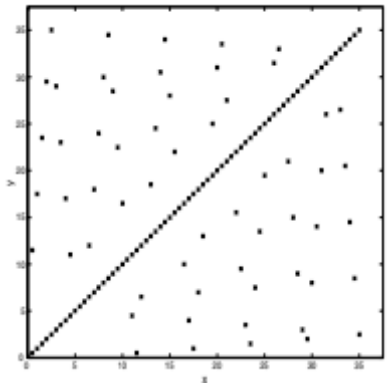
$$x \not\equiv y \pmod N.$$

Αυτό είναι ένα πρόβλημα ελαχιστοποίησης 2 διαστάσεων και το ολικό ελάχιστο της συνάρτησης g είναι 0. Για λόγους ευκολίας , θα ονομάζουμε το πρόβλημα ελαχιστοποίησης της συνάρτησης g , π.χ. την εύρεση ενός ολικού ελάχιστου (x^* ,y^*) της συνάρτησης g που υπόκειται στον περιορισμό $x \not\equiv y \pmod N$,

ως Πρόβλημα 1.



Η γραφική παράσταση της συνάρτησης $g(x,y) = x^2 - y^2 \pmod{N}$, για N= 143.



Η καμπύλη συνάρτησης περιγράμματος της συνάρτησης g στο ολικό ελάχιστο g(x,y) =0 , για N=143 και g=0.

4.2.2 2ο <u>Πρόβλημα</u>

Ορίζουμε την συνάρτηση ελαχιστοποίησης h : { 1,2,..,N-1}→ {0,1,..,N-1 } με

$$h(x) = (x-a)(x-b) \pmod{N},$$

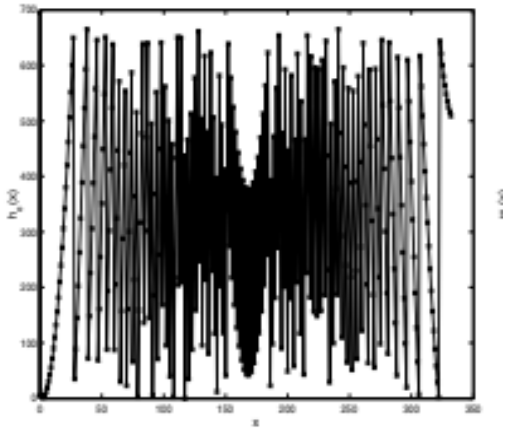
Όπου a,b είναι μη μηδενικοί ακέραιοι και

$$x \not\equiv a \pmod{N},\ x \not\equiv b \pmod{N}$$

Μία δοκιμαστική περίπτωση του προβλήματος είναι η συνάρτηση :

$$h_e(x) = (x-1)(x-2) \pmod{N},$$

όπου $x \neq 1 \pmod{N}$ και $x \neq 2 \pmod{N}$. Αυτό είναι ένα 1-διάστασης πρόβλημα ελαχιστοποίησης με ολικό ελάχιστο το μηδέν. Θα αναφερόμαστε στην ελαχιστοποίηση της συνάρτησης $h_e(x)$, που υπόκειται στους περιορισμούς $x \neq 1 \pmod{N}$ και $x \neq 2 \pmod{N}$, ως Πρόβλημα 2.



Η συνάρτηση $h_e(x)$ για μικρή αξία N=23 *29=667.

Σε γενικότερο πλαίσιο, μπορούμε να θεωρήσουμε την ελαχιστοποίηση της συνάρτησης

$$w(x) = (x-a)(x-b)\cdots(x-m) \pmod N,$$

Όπου x ∈ {0,1,…,N-1} και

$$x \not\equiv \{a, b, \ldots, m\} \pmod N.$$

4.2.3 3ο Πρόβλημα

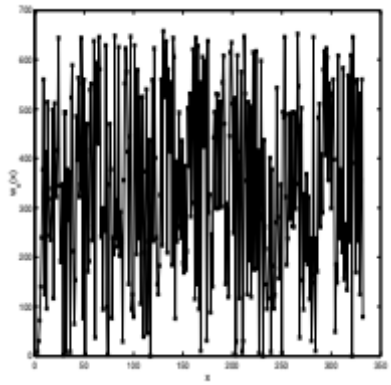
Μελετάμε την περίπτωση :

$$w_e(x) = (x+1)(x-1)(x-2) \pmod N,$$

$$x \not\equiv \{-1, 1, 2\} \pmod N.$$

Ονομάζουμε Πρόβλημα 3 την 1-διάστασης ελαχιστοποίηση της συνάρτησης $w_e(x)$ με περιορισμούς

$$x \not\equiv \{-1, 1, 2\} \pmod N,$$



Γραφική παράσταση της $w_e(x)$ για N= 23*29=667.

4.3 Πειραματική Εκτέλεση και αποτελέσματα.

Θα εφαρμοστούν οι PSO και η DE στα προβλήματα 1,2,3 που παρουσιάστηκαν στο 4.1 και συγκρίνονται με την απλή τεχνική τυχαίας αναζήτησης. Χρησιμοποιούνται η ολική και η τοπική PSO μέθοδος και των δύο περιπτώσεων, των βαρών και του παράγοντα στένωσης , όπως και οι παραλλαγές της DE με τους μηχανισμούς μετάλλαξης. Οι τυπικές αξίες παραμέτρου για τις παραλλαγές της PSO χρησιμοποιούνται και η τοπική εκδοχή της PSO δοκιμάζεται για μέγεθος

γειτονιάς ίσο με 1. Όσο αφορά την PSO, τα προκαταρτικά πειράματα σε αυτά τα προβλήματα έδειξαν ότι η αξία της μέγιστης ταχύτητας V_{max} των σωματιδίων επηρεάζει σημαντικά την απόδοση του. Για το πρόβλημα 1,τα πιο υποσχόμενα αποτελέσματα παράχθηκαν χρησιμοποιώντας τις αξίες V_{max} = ((N-7)/10,(N-7/10) και για τα προβλήματα 2,3 η V_{max} =(N-4)/5 .Οι παράμετροι για τον αλγόριθμο DE είναι οι F=0.5 και CR= 0.5. Σε όλες τις περιπτώσεις, οι πληθυσμοί περιορίζονται να είναι στην εφικτή περιοχή του προβλήματος.

Για το πρόβλημα 1,την ελαχιστοποίηση της g δηλαδή, οι μέθοδοι ερευνώνται για πολλές αξίες του N, στο εύρος N= 199 x 211= 41989 ως N= 691 x 701= 484391. Για κάθε αξία της N 100 ανεξάρτητοι γύροι πραγματοποιούνται. Τα αποτελέσματα είναι στον ακόλουθο πίνακα. Στον πίνακα, PSOGW είναι η ολική εκδοχή της PSO με βάρη αδράνειας, PSOGC η PSO με παράγοντα στένωσης , PSOLW η τοπική PSO με βάρη αδράνειας , PSOLC, η τοπική PSO με παράγοντα στένωσης. DE1 η DE με μηχανισμό μετάλλαξης όπως η 1.5 και DE2 όπως η 1.8. Η τυχαία έρευνα (Random Search) σημειώνεται ως RS. Ένας γύρος σημειώνεται ως επιτυχημένος αν ο αλγόριθμος εντοπίσει ένα ολικό ελάχιστο μέσα σε έναν προκαθορισμένο αριθμό αξιολογήσεων της συνάρτησης.

N	Method	Suc.Rate	mean F.E.	St.D. F.E.	median F.E.	min F.E.
	PSOGW	56%	8844.643	5992.515	8325.000	660
	PSOGC	48%	7149.375	5272.590	5355.000	330
	PSOLW	51%	8329.412	6223.142	7050.000	270
$N = 199 \times 211$	PSOLC	51%	7160.588	6001.276	5940.000	420
	DE1	4%	517.500	115.866	465.000	450
	DE2	9%	5476.667	6455.651	1830.000	60
	RS	66%	9104.015	5862.358	8700.500	22
	PSOGW	41%	16210.244	11193.375	15090.000	120
	PSOGC	45%	16818.667	12664.632	13800.000	630
	PSOLW	58%	18455.690	12870.897	14520.000	270
$N = 293 \times 307$	PSOLC	50%	16374.000	13597.782	13365.000	120
	DE1	7%	1598.571	1115.488	1470.000	120
	DE2	19%	17815.263	12484.580	16290.000	2730
	RS	64%	21548.531	13926.751	20852.500	57
	PSOGW	53%	31965.849	24423.975	27570.000	780
	PSOGC	45%	32532.667	22652.983	33210.000	1740
	PSOLW	55%	31472.182	23394.791	22620.000	720
$N = 397 \times 401$	PSOLC	54%	38156.111	22925.970	37665.000	750
	DE1	1%	1680.000	0.000	1680.000	1680
	DE2	12%	27722.500	17498.736	28620.000	180
	RS	60%	27302.567	21307.031	23607.500	145
	PSOGW	56%	49893.750	37515.327	44640.000	930
	PSOGC	55%	49975.636	36727.380	41760.000	300
	PSOLW	55%	49207.091	34053.904	50430.000	2010
$N = 499 \times 503$	PSOLC	46%	48443.478	34677.039	43470.000	1920
	DE1	1%	2480.000	0.000	2480.000	2480
	DE2	8%	67245.000	35114.316	64770.000	14730
	RS	61%	54139.443	38642.970	48743.000	140
	PSOGW	52%	72175.000	48653.823	71550.000	600
	PSOGC	51%	81476.471	53666.543	75100.000	5000
	PSOLW	49%	78651.020	48197.105	67400.000	11200
$N = 599 \times 601$	PSOLC	52%	69542.308	48837.949	53050.000	2500
	DE1	2%	4700.000	4808.326	4700.000	1300
	DE2	5%	8620.000	8078.180	9300.000	800
	RS	64%	86123.656	47504.284	89392.500	904
	PSOGW	46%	207443.478	163585.340	214800.000	800
	PSOGC	46%	175426.086	138118.794	149200.000	800
	PSOLW	60%	196993.334	146204.518	144500.000	9200
$N = 691 \times 701$	PSOLC	52%	209307.692	163833.606	200100.000	1800
	DE1	2%	23800.000	25000.000	23800.000	21000
	DE2	10%	71000.000	95357.642	15200.000	1600
	RS	60%	185932.334	126355.926	154999.000	2828

Οι μεταβλητές της PSO ξεπερνάνε σε τιμές επιτυχίας αυτές της μεθόδου DE. Η απόδοση της DE πέφτει όσο ανεβαίνει η τιμή του N ενώ όσο αφορά αυτό τον παράγοντα, η PSO παραμένει πιο σταθερή. Ωστόσο, σε αντίθεση με όσα είναι γνωστά, τα καλύτερα ποσοστά επιτυχίας των μεθόδων τεχνητής νοημοσύνης είναι σχετικά χαμηλά (περίπου 50%), ενώ η RS τα ξεπερνά. Αυτό δείχνει ότι η σχεδόν τυχαία συμπεριφορά του συγκεκριμένου είδους προβλήματος καθιστά δύσκολο για τις μεθόδους EC να εξορύξουν πληροφορίες για την δυναμική του. Στις περιπτώσεις που οι μέθοδοι EC εντοπίζουν ένα ολικό ελάχιστο χρειάζονται μικρότερο αριθμό αξιολογήσεων της συνάρτησης, σεβόμενες τον κύριο τομέα της συνάρτησης. Όπου οι Όπου οι EC μέθοδοι απέτυχαν στην εύρεση ολικού ελάχιστου, εντόπισαν τοπικό με τιμή κοντά σε αυτή του ολικού.

Παρόμοια αποτελέσματα εξάγονται για τα προβλήματα 2 και 3, ελαχιστοποίηση συνάρτησης h_e και w_e αντίστοιχα, και για N=103 x 107 και παρουσιάζονται στον παρακάτω πίνακα. Για το πρόβλημα 3, οι επιτυχίες της μεθόδου PSO είναι υψηλές (περίπου 80%), ενώ η απόδοση της DE παραμένει χαμηλά. Ωστόσο, η RS πάλι τις ξεπερνά.

Function	Method	Suc.Rate	mean F.E.	St.D. F.E.	median F.E.	min F.E.
	PSOGW	51%	2013.333	1483.535	1500.000	100
	PSOGC	57%	1974.035	1609.228	1420.000	60
	PSOLW	59%	1677.288	1254.688	1420.000	60
h_e	PSOLC	58%	2385.862	1676.898	2040.000	120
	DE1	1%	100.000	0.000	100.000	100
	DE2	1%	80.000	0.000	80.000	80
	RS	65%	2099.646	1448.007	2056.000	6
	PSOGW	79%	1382.785	1265.927	820.000	40
	PSOGC	84%	1402.857	1442.194	930.000	40
	PSOLW	80%	1757.750	1544.267	1110.000	40
w_e	PSOLC	85%	1416.000	1329.034	880.000	40
	DE1	1%	60.000	0.000	60.000	60
	DE2	1%	80.000	0.000	80.000	80
	RS	96%	1507.969	1328.913	1104.000	7

4.4 Κρυπτανάλυση Feistel Cipher με μεθόδους Εξελεκτικού Υπολογισμού. (EC)

Σε αυτό το κεφάλαιο, η Διαφορική Κρυπτανάλυση ενός κρυπτοσυστήματος Feistel θα μελετηθεί ως Πρόβλημα βελτιστοποίησης. Συγκεκριμένα, το πρόβλημα εύρεσης χαμένων bit του κλειδιού που χρησιμοποιείται σε ένα απλό Feistel κρυπτογράφημα, ονομάζεται Data Encryption Standard με τέσσερις ή έξι γύρους, είναι οι δύο κατηγορίες στις οποίες κατηγοριοποιούνται όλα τα προβλήματα που ψάχνουμε bit.

Θα μελετηθεί η εφαρμογή PSO και DE σε τέτοια προβλήματα. Τα αποτελέσματα έδειξαν ότι η DES τεσσάρων γύρων εντοπίζει την λύση αποτελεσματικά, καθώς απαιτεί λιγότερο αριθμό αξιολογήσεων της συνάρτησης συγκρινόμενη με την επίθεση ωμής βίας. Για την DES έξι γύρων, η αποτελεσματικότητα εξαρτάται από την δομή της αντικειμενικής συνάρτησης.

4.4.1 Διατύπωση του προβλήματος.

4.4.1.1 DES 4 Επαναλήψεων

Για την DES 4 επαναλήψεων, η DC (Differential Cryptanalysis-Διαφορική Κρυπτανάλυση) χρησιμοποιεί ένα χαρακτηριστικό μιας επανάληψης που συμβαίνει με πιθανότητα 1, που έχει ανακτηθεί από το πρώτο βήμα της κρυπτανάλυσης 42 bits του δευτερεύοντος κλειδιού του

τελευταίου γύρου. Υπολογίζοντας την περίπτωση όπου τα δευτερεύοντα κλειδιά υπολογίζονται με τον αλγόριθμο προγραμματισμού DES, τα 42 bits που δίνονται από την DC είναι τα πραγματικά bits του κλειδιού και υπάρχουν και 14 bits που υπολείπονται για την ολοκλήρωση του κλειδιού. Η επίθεση ωμής βίας απαιτεί 2^{14} δοκιμές. Το σωστό κλειδί πρέπει να ικανοποιεί τη XOR αξία του γνωστού κειμένου για όλα τα ζευγάρια που χρησιμοποιούνται στην DC. Μία διαφορετική προσέγγιση είναι να χρησιμοποιηθεί ένα δεύτερο χαρακτηριστικό που ανταποκρίνεται στα bits που ψάχνουμε και να γίνει μία προσπάθεια για πιο προσεκτικό υπολογισμό των bits το κλειδιού των τελευταίων δύο γύρων, που είναι όμως πιο περίπλοκο.

Αντί να χρησιμοποιούμε αυτούς τους τρόπους, μετατρέπουμε το πρόβλημα σαν ακέραιο πρόβλημα βελτιστοποίησης. Εφόσον το σωστό κλειδί ικανοποιεί την XOR αξία του γνωστού απλού κειμένου για όλα τα ζευγάρια που χρησιμοποιούνται από την DC, τα κρυπτοκείμενα μπορούν να χρησιμοποιηθούν για την αξιολόγηση των πιθανών λύσεων που δίνονται από τις μεθόδους βελτιστοποίησης. Έτσι, το X γίνεται ένα διάνυσμα 14-διαστάσεων, όπου κάθε ένα από τα συστατικά του, ανταποκρίνεται σε ένα από τα 14 άγνωστα bits του κλειδιού. Κάθε τέτοιο διάνυσμα είναι μία πιθανή λύση του προβλήματος βελτιστοποίησης. Ας είναι το np ο αριθμός των κρυπτογραφημένων ζευγών που χρησιμοποιεί η DC για να αποκτήσει τα σωστά 42 bits του κλειδιού. Έτσι, μπορούμε να κατασκευάσουμε τα 56 bits του κλειδιού, χρησιμοποιώντας τα 42 που ανακτήθηκαν από την DC τα 14 συστατικά του X σε σωστή σειρά. Με το κλειδί που προκύπτει, αποκρυπτογραφούμε τα np κρυπτογραφημένα ζεύγη και υπολογίζουμε τον αριθμό των κρυπτογραφημένων ζευγών που ικανοποιούν την XOR αξία του γνωστού μη κρυπτογραφημένου κειμένου, που ονομάζουμε cnpx. Η αντικειμενική συνάρτηση f είναι η διαφορά μεταξύ της επιθυμητής εκροής np και της πραγματικής, cnp_x ,πχ $f(X)= np-cnp_x$. Το ολικό ελάχιστο της f είναι 0 και ο ολικός ελαχιστοποιητής είναι με μεγάλη πιθανότητα το πραγματικό κλειδί.

4.4.1.2 DES 6 Επαναλήψεων

Η κρυπτανάλυση με 6 επαναλήψεις είναι πιο περίπλοκη από αυτή με τις 4, και το καλύτερο χαρακτηριστικό που μπορεί να χρησιμοποιηθεί έχει πιθανότητα μικρότερη του 1. Συγκεκριμένα, η DC χρησιμοποιεί δύο χαρακτηριστικά πιθανότητας p_{sr} =1/16 για να εφοδιάσει τα 42 bits του σωστού κλειδιού. Και πάλι, υπολείπονται 14 bits. Σε αυτή τη περίπτωση, το σωστό κλειδί μπορεί να μη προτείνεται από όλα τα κρυπτογραφημένα ζεύγη. Αυτό συμβαίνει γιατί μπορεί να μην είναι όλα τα ανταποκρινόμενα ζεύγη απλού κειμένου τα κατάλληλα ζεύγη. Ένα ζεύγος ονομάζεται *σωστό – right* υπακούοντας σε ένα r-round χαρακτηριστικό $\Omega=(\Omega_P, \Omega_\Lambda , \Omega_C)$ και ένα ανεξάρτητο κλειδί K, αν ισχύει $P'=\Omega_P$, όπου P' είναι η XOR αξία του ζεύγους και για τους πρώτους r γύρους της κρυπτογράφησης του ζεύγους χρησιμοποιώντας το ανεξάρτητο κλειδί K η εισροή και η εκροή XOR's της ith επανάληψης ισούνται με λ_I^i και λ_O^i αντίστοιχα.

Η πιθανότητα ένα ζεύγος με απλό κείμενο XOR να ισούται με Ω_P του χαρακτηριστικού είναι ένα σωστό ζεύγος που χρησιμοποιεί ένα προκαθορισμένο κλειδί είναι περίπου ίση με την πιθανότητα του χαρακτηριστικού. Ένα μη σωστό ζεύγος λέγεται *λάθος-wrong* ζεύγος και δεν προτείνει κατά ανάγκη το σωστό κλειδί ως πιθανή τιμή. Η μελέτη σωστών και λάθος κλειδιών, έδειξαν ότι το σωστό κλειδί εμφανίζεται με την πιθανότητα των χαρακτηριστικών από τα σωστά ζεύγη και κάποια τυχαία από τα λάθος ζεύγη. Συμπερασματικά, αν όλα τα ζεύγη (σωστά και λάθος) της DC χρησιμοποιούνται στην προκαθορισμένη αντικειμενική συνάρτηση f, η ελάχιστη αξία της συνάρτησης θα αλλάζει ανάλογα με τα συγκεκριμένα ζεύγη που χρησιμοποιούνται. Αν τα σωστά ζεύγη φιλτράρονται και είναι τα μόνα που χρησιμοποιούνται στην αντικειμενική συνάρτηση f, το ολικό ελάχιστο της συνάρτησης θα είναι συνεχώς ίσο με 0, όπως στην περίπτωση των bits που ψάχνουμε στον DES 4 επαναλήψεων. Καθώς το φιλτράρισμα αυτό δεν είναι πάντα εφικτό, μελετάμε την προσέγγιση όπου χρησιμοποιούμε στην συνάρτηση όλα τα ζεύγη της DC.

4.4.1.3 Μορφοποίηση του προβλήματος και Αποτελέσματα.

Και οι δύο μέθοδοι, PSO και DE, θεωρούν κάθε συστατικό της πιθανής λύσης ως έναν πραγματικό αριθμό στο εύρος [0,1] και όλοι οι πληθυσμοί περιορίζονται να είναι στην εφικτή περιοχή του προβλήματος. Για την αξιολόγηση των προτεινόμενων λύσεων, εφαρμόστηκε η τεχνική της ολοκλήρωσης των πραγματικών τιμών του προβλήματος στον κοντινότερο ακέραιο. Για τη μέθοδο PSO λάβαμε υπόψη και τις ολικές και τις τοπικές μεταβλητές, και για τον DE αλγόριθμο τις πέντε μεταβλητές που αναλύθηκαν παραπάνω. Ορίστηκε μία μέγιστη αξία για την ταχύτητα, V_{max} =0,5, στην PSO, για να αποφευχθεί η καταστροφή της δυναμικής της μεθόδου, για παράδειγμα αν πάρουν οι ταχύτητες μεγάλες τιμές, τα σωματίδια θα βγουν εκτός της περιοχής έρευνας. Οι παράμετροι της PSO ορίζονται σε προκαθορισμένες τιμές, π.χ. χ=0.729, c1=c2=2.05 και οι παράμετροι της DE ορίστηκαν σε τιμές CR=F=0,5.

Η προτεινόμενη προσέγγιση εξετάστηκε για διάφορα πιθανά κλειδιά και νούμερα ζευγαριών, np.Για κάθε δοκιμή, το μέγεθος του πληθυσμού ήταν 100 και η μέθοδος ερευνήθηκε σε 100 ανεξάρτητους γύρους. Ένας γύρος θεωρείται επιτυχής αν ο αλγόριθμος εντοπίζει το ολικό ελάχιστο μέσα σε ένα προκαθορισμένο αριθμό αξιολογήσεων της συνάρτησης. Το κατώφλι της αξιολόγησης της συνάρτησης ήταν το 2^{14}.

Για τα bits που ψάχνουμε με την DES μειωμένη σε 4 γύρους, τα αποτελέσματα για 6 διαφορετικά κλειδιά, k_i , i=1,2,..6 και για ζευγάρια έρευνας np, 20 και 50, τα αποτελέσματα φαίνονται αντίστοιχα στους πίνακες στους δύο πρώτους πίνακες και για DES έξι γύρων με np=200 και για τα ίδια 6 κλειδιά, τα αποτελέσματα είναι στον τελευταίο πίνακα.

key	Method	Suc.Rate	Mean F.E.
	PSOGC	99%	742.42
	PSOLC1	100%	1773.00
	PSOLC2	100%	1255.00
	DE1	100%	614.00
k_1	DE2	100%	1406.00
	DE3	100%	780.00
	DE4	100%	588.00
	DE5	100%	1425.00
	PSOGC	99%	911.11
	PSOLC1	100%	2665.00
	PSOLC2	100%	1650.00
	DE1	100%	603.00
k_2	DE2	100%	1518.00
	DE3	100%	879.00
	DE4	100%	615.00
	DE5	100%	1649.00
	PSOGC	94%	1117.02
	PSOLC1	99%	2447.48
	PSOLC2	100%	1688.00
	DE1	99%	693.94
k_3	DE2	100%	1497.00
	DE3	100%	805.00
	DE4	100%	690.00
	DE5	100%	1427.00
	PSOGC	96%	876.04
	PSOLC1	100%	2089.00
	PSOLC2	100%	1418.00
	DE1	99%	701.01
k_4	DE2	100%	1378.00
	DE3	100%	843.00
	DE4	100%	568.00
	DE5	100%	1362.00

	PSOGC	97%	900.00
	PSOLC1	99%	1979.80
	PSOLC2	100%	1496.00
	DE1	100%	662.00
k_5	DE2	100%	1493.00
	DE3	100%	848.00
	DE4	100%	662.00
	DE5	100%	1542.00
	PSOGC	93%	1457.00
	PSOLC1	95%	4475.79
	PSOLC2	99%	2913.13
	DE1	100%	651.00
k_6	DE2	100%	1717.00
	DE3	100%	1063.00
	DE4	99%	725.25
	DE5	100%	1583.00

np=20 ζευγάρια

key	Method	Suc.Rate	Mean F.E.
	PSOGC	99%	860.61
	PSOLC1	100%	1698.00
	PSOLC2	100%	1141.00
	DE1	100%	485.00
k_1	DE2	100%	1215.00
	DE3	100%	785.00
	DE4	100%	553.00
	DE5	100%	1382.00
	PSOGC	94%	741.49
	PSOLC1	100%	1367.00
	PSOLC2	100%	1100.00
	DE1	99%	490.91
k_2	DE2	100%	1081.00
	DE3	100%	669.00
	DE4	100%	521.00
	DE5	100%	1128.00
	PSOGC	99%	631.31
	PSOLC1	100%	1217.00
	PSOLC2	100%	1035.00
	DE1	100%	385.00
k_3	DE2	100%	1006.00
	DE3	100%	546.00
	DE4	100%	409.00
	DE5	100%	1016.00
	PSOGC	90%	947.78
	PSOLC1	98%	2292.88
	PSOLC2	100%	1588.00
	DE1	98%	666.33
k_4	DE2	100%	1342.00
	DE3	100%	838.00
	DE4	99%	649.50
	DE5	100%	1294.00
	PSOGC	100%	707.00
	PSOLC1	100%	1763.00
	PSOLC2	100%	1193.00
	DE1	100%	445.00
k_5	DE2	100%	1127.00
	DE3	100%	684.00
	DE4	100%	465.00
	DE5	100%	1131.00

	PSOGC	96%	880.21
	PSOLC1	100%	2009.00
	PSOLC2	100%	1390.00
	DE1	100%	507.00
k_6	DE2	100%	1250.00
	DE3	100%	692.00
	DE4	100%	563.00
	DE5	100%	1230.00

np= 50 ζεύγη

key	Method	Suc.Rate	Mean F.E.
	PSOGC	26%	7038.46
	PSOLC1	9%	2188.89
	PSOLC2	8%	3862.50
	DE1	36%	5191.67
k_1	DE2	52%	5515.39
	DE3	41%	5807.32
	DE4	51%	6364.71
	DE5	59%	6855.93
	PSOGC	24%	5037.50
	PSOLC1	3%	1500.00
	PSOLC2	7%	2357.14
	DE1	34%	6535.29
k_2	DE2	58%	6968.97
	DE3	40%	5945.00
	DE4	39%	6897.44
	DE5	61%	6932.79
	PSOGC	41%	4902.44
	PSOLC1	6%	4533.33
	PSOLC2	5%	7340.00
	DE1	48%	5070.83
k_3	DE2	61%	6967.21
	DE3	53%	6698.11
	DE4	48%	5889.58
	DE5	56%	7926.79
	PSOGC	47%	4912.77
	PSOLC1	13%	4407.69
	PSOLC2	23%	4134.78
	DE1	57%	6491.23
k_4	DE2	76%	7594.74
	DE3	66%	6418.18
	DE4	72%	5741.67
	DE5	76%	7001.32
	PSOGC	36%	5575.00
	PSOLC1	4%	1950.00
	PSOLC2	5%	4700.00
	DE1	51%	5688.24
k_5	DE2	62%	7803.23
	DE3	57%	5229.83
	DE4	53%	5377.36
	DE5	64%	6387.50
	PSOGC	37%	5624.32
	PSOLC1	5%	2920.00
	PSOLC2	9%	3377.78
	DE1	49%	5681.63
k_6	DE2	63%	7380.95
	DE3	50%	7048.00
	DE4	51%	5621.57
	DE5	64%	7679.69

np= 200 ζεύγη

Επεξηγήσεις.

PSOCG: PSO με παράγοντα στένωσης

PSOCL1: PSO με μέγεθος γειτονιάς ίσο με 1

PSOCL2: PSO με μέγεθος γειτονιάς ίσο με 2

DE1, DE2 DE3, DE4, DE5: οι 5 εκδοχές της DE

Suc. Rate : Success rate, το ποσοστό στο οποίο κάθε αλγόριθμος βρήκε το ολικό ελάχιστο εντός του προκαθορισμένου κατωφλίου
Mean F.E. : Μέση τιμή των αξιολογήσεων της συνάρτησης. (Function Evaluations)

4.4.2 Παρατηρήσεις

Τα ποσοστά επιτυχίας και των δύο μεθόδων για όλες τις εκδοχές είναι υψηλά. Για np=20 τα ποσοστά είναι 93%-100% , με μέσο όρο το 99,3% και για np=50 είναι μεταξύ 90%-100% με μέσο το 99,4%. Η βελτίωση του ποσοστού επιτυχίας όσο μεγαλώνει ο αριθμός των ζευγών np είναι αναμενόμενη, εφόσον ο μεγαλύτερος αριθμός των ζευγαριών που χρησιμοποιούνται για την αξιολόγηση των πιθανών λύσεων, μειώνει την πιθανότητα μίας λάθους πλειάδας 14 bits να προταθεί ως η σωστή. Ο μέσος αριθμός των αξιολογήσεων της συνάρτησης που απαιτούνται για να εντοπιστεί το ολικό ελάχιστο είναι για np=20, 1309 και για np=50, 982. Αυτό υποδηλώνει ότι όσα περισσότερα ζευγάρια κρυπτοκειμένου εμπλέκονται στην συνάρτηση, όχι μόνο η αξιολόγηση γίνεται πιο ακριβής, αλλά και το ολικό ελάχιστο εντοπίζεται ευκολότερα. Ωστόσο, ο αριθμός των ζευγών κρυπτοκειμένου της προτεινόμενης προσέγγισης δεν πρέπει να ξεπερνά τον αριθμό των ζευγών που χρησιμοποιούνται από την DC για το αρχικό πρόβλημα, γιατί αυτό θα αύξανε το συνολικό κόστος της κρυπτανάλυσης σε κρυπτογραφήσεις και αποκρυπτογραφήσεις.

DES 4 Επαναλήψεων

PSO

Η PSOLC2 , πετυχαίνει ποσοστά κοντά στο 100%, σε όλες τις περιπτώσεις του πρώτου προβλήματος, με μέσο όρο αριθμού αξιολογήσεων συνάρτησης 1489. Η PSOGC ποσοστά 93%-100% , με 898 αξιολογήσεις περίπου. Αυτό σημαίνει ότι αν και η PSOGC έχει χαμηλότερα ποσοστά επιτυχίας, στις περιπτώσεις όπου και η local και η global PSO μπορούν να εντοπίσουν το ελάχιστο, η PSOGC χρειάζεται λιγότερες επαναλήψεις.

DES

Οι εκδοχές της DES έχουν μια σταθερή και παρόμοια συμπεριφορά, με μέσο ποσοστό επιτυχίας το 100% σε όλες τις περιπτώσεις. Μόνο η DE4 έχει 99% σε δύο περιπτώσεις. Η DE1 έχει τον χαμηλότερο βαθμό αξιολογήσεων από όλες τις μεθόδους και τις εκδοχές τους.

DES 6 Επαναλήψεων

Σε αυτή την περίπτωση, χρησιμοποιούμε σωστά και λάθος ζεύγη για την κατασκευή της αντικειμενικής συνάρτησης, βλέπουμε ότι υπάρχουν μεγάλες διαφορές στα ποσοστά επιτυχίας σε σχέση με την DES 4 επαναλήψεων. Αυτό αποδίδεται στο γεγονός ότι στην προηγούμενη περίπτωση δουλεύουμε με ένα χαρακτηριστικό που προκύπτει με πιθανότητα 1 ενώ στην τελευταία με ένα χαρακτηριστικό μ μικρότερη (1/16). Αυτό σημαίνει ότι στα 200 ζευγάρια κρυπτοκειμένων περίπου, που χρησιμοποιούνται από την αντικειμενική συνάρτηση, τα 12 είναι σωστά και προτείνουν τη σωστή πλειάδα και τα υπόλοιπα 188 κάνουν τυχαίες προτάσεις, μειώνοντας την πιθανότητα της πρότασης του σωστού. Εφόσον η αντικειμενική συνάρτηση γίνεται πιο αποτελεσματική όταν περισσότερα σωστά ζεύγη είναι διαθέσιμα ή όταν η πιθανότητα του χρησιμοποιούμενου χαρακτηριστικού είναι μεγάλη, είναι αναμενόμενο ότι η εφαρμογή των μεθόδων στη περίπτωση των 4 γύρων να είναι καλύτερη από των έξι. Η PSOGC και όλες οι DE περιπτώσεις εντόπισαν τα χαμένα bits με μέσο 35% ανεξάρτητων γύρων για την PSOGC και 55%

για την DE και για τα έξι κλειδιά που δοκιμάστηκαν. Ο μέσος όρος αξιολογήσεων της συνάρτησης είναι 5600.

Στην DES 4 επαναλήψεων όλες οι μέθοδοι σε ανεξάρτητες δοκιμές εντοπίζουν τέσσερες διαφορετικές πλειάδες 14 bits ικανοποιώντας το κριτήριο συνθήκης της αντικειμενικής συνάρτησης. Αυτές οι 4 λύσεις του προβλήματος βρίσκονται σε δύο προκαθορισμένες θέσεις, την $10^{η}$ και την $36^{η}$ του κλειδιού της DES. Στην DES των 6 γύρων μόνο 1 λύση, η σωστή εντοπίστηκε από όλες τις μεθόδους..

Η προτεινόμενη μεθοδολογία είναι αποτελεσματική για την επίλυση τέτοιου είδους προβλήματα , εφόσον η DES 4 επαναλήψεων χρειάζεται περίπου 576 αξιολογήσεις συνάρτησης σε αντίθεση με την επίθεση ωμής βίας που απαιτεί 2^{14} =16384 αξιολογήσεις. Επίσης κρίνοντας από τα αποτελέσματα, η αποτελεσματικότητα της DES 6 γύρων βασίζεται στην κατασκευή της αντικειμενικής συνάρτησης. Η αποτελεσματικότητα της μεθόδου, παρουσιάζει ενδιαφέρον για το κατά πόσο θα είναι αποτελεσματική σε bits κλειδιών κρυπτογραφημάτων Feistel.

ΚΕΦΑΛΑΙΟ 5ο : ΤΑ ΤΕΧΝΗΤΑ ΝΕΥΡΩΝΙΚΑ ΔΙΚΤΥΑ ΣΤΗΝ ΚΡΥΠΤΑΝΑΛΥΣΗ.

Σε αυτό το κεφάλαιο θα παρουσιαστεί η χρήση των ΤΝΔ στην κρυπτανάλυση. Αρχικά, θα παρουσιαστεί η κρυπτανάλυση κλασσικών κρυπτογραφημάτων, με ΤΝΔ που εντοπίζουν τις αδυναμίες των δικτύων και αποκαλύπτουν το κλειδί κρυπτογράφησης, έτσι ώστε το δίκτυο να μπορέσει να προβλέψει το κλειδί οποιοδήποτε πιθανού κρυπτογραφήματος.

5.1 Κρυπτανάλυση Κλασσικών Κρυπτογραφημάτων.

Τα κρυπτογραφήματα που θα παρουσιαστούν είναι μεν απλά και εύκολα στην κρυπτανάλυση, αλλά σκοπός είναι να παρουσιαστεί και να κατανοηθεί η μέθοδος εκπαίδευσης των ΤΝΔ. Ορίζουμε ένα σύνολο απλών κειμένων P, ένα σύνολο κρυπτοκειμένων C και ένα σύνολο κλειδιών K. Θα αναλυθούν τα παρακάτω κρυπτογραφήματα.

Το κρυπτογράφημα του Καίσαρα είναι ένα μονοαλφαβητικό κρυπτογράφημα που αναπαριστά ένα γράμμα του απλού κειμένου κάθε φορά με ένα του κρυπτοκειμένου.

Ορισμός 1. Δοθέντος ενός απλού κειμένου x∈ P, ένα κρυπτοκείμενο y∈ C και ένα κλειδί k∈K , όπου $P=C=K=Z_{26}$, ένα κρυπτογράφημα Καίσαρα ορίζεται από την συνάρτηση E_k (x)= x + kmod26 και η συνάρτηση αποκρυπτογράφησης D_k (y) =y – kmod26. Ο αριθμός των διαφορετικών κλειδιών περιορίζεται στο 26 (τιμές μεταξύ 0 και 25), οπότε είναι εφικτή μία δοκιμαστική επίθεση ωμής βίας.

Το κρυπτογράφημα Vigenere είναι ένα πολύ-αλφαβητικό κρυπτογράφημα που αναπαριστά κάθε γράμμα του κειμένου που θέλουμε να κρυπτογραφήσουμε με ένα σύνολο διαφορετικών γραμμάτων. Το κρυπτογράφημα δουλεύει σε μπλοκ m γραμμάτων με κλειδί μήκους m.

Ορισμός 2 Δοθέντος ενός απλού κειμένου x∈ P, ένα κρυπτοκειμένου y∈ C και ένα κλειδί k∈K , όπου $P=C=K=Z^m{}_{26}$ και $Z^m{}_{26}$ είναι Z_{26} x Z_{26} x…. x Z_{26} ,m φορές, για ένα κλειδί K= (k_1, ..,k_m) , το κρυπτογράφημα Vigenere ορίζεται από την συνάρτηση κρυπτογράφησης $E_{k1,..km}$ (x_1,..,x_m) = (x_1 +k_1 ,x_m +k_m) mod26 και τη συνάρτηση αποκρυπτογράφησης $D_{k1,..km}$ (y_1,..,y_m) = y_1 –k_1 ,..,y_m –k_m)mod26.

Ο αριθμός των πιθανών κλειδιών είναι 26^m .

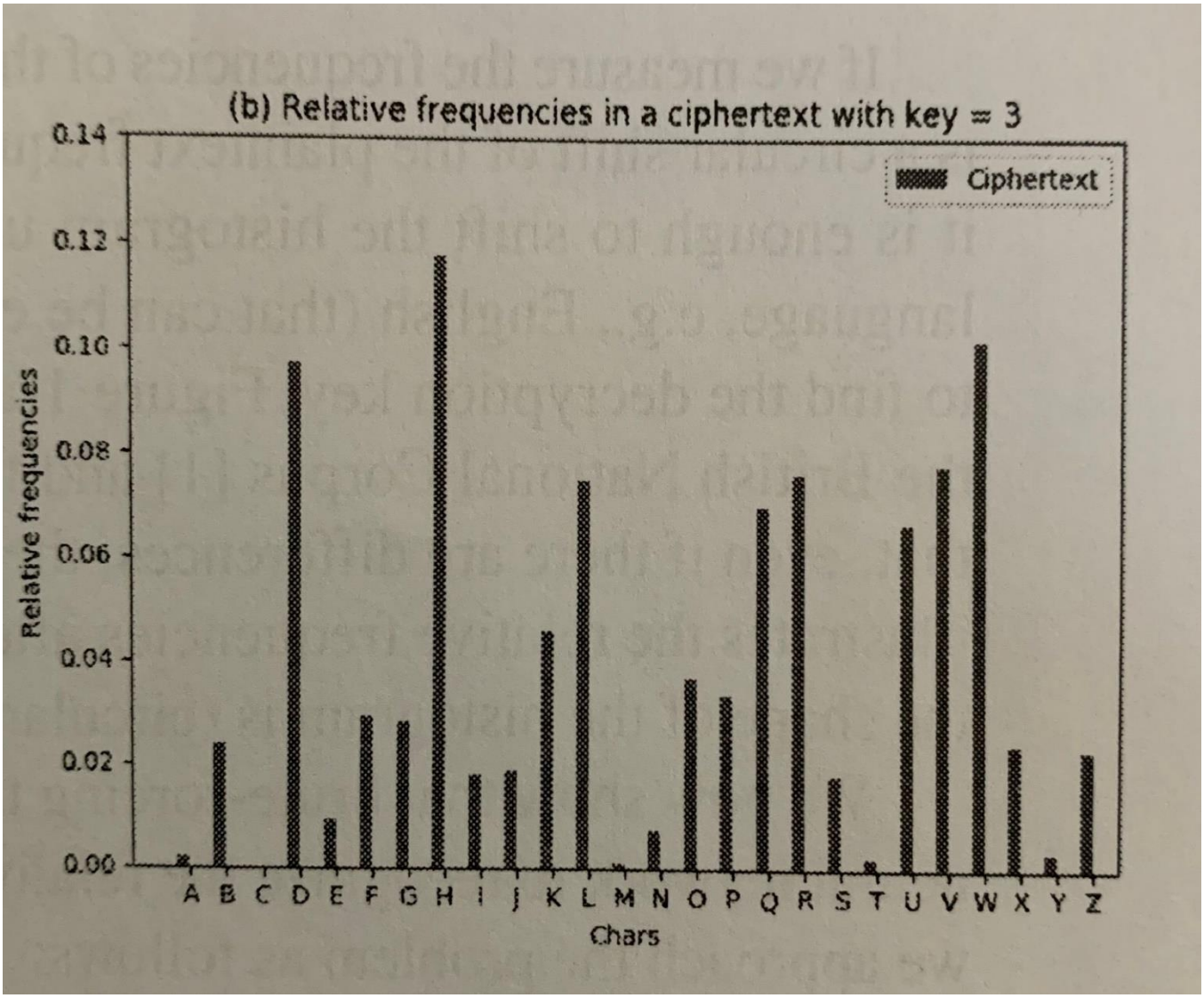
Ένα υποκατάστατο κρυπτογράφημα είναι ένα μονοαλφαβητικό κρυπτογράφημα που μετατρέπει τα γράμματα της αλφαβήτου σε μία γενική μετάθεση.

Ορισμός 3: Δοθέντος ενός απλού κειμένου x∈ P, ένα κρυπτοκειμένου y∈ C και ένα κλειδί p∈K , όπου P=C=Z_{26} και K={p | p είναι μία μετάθεση 0,1,..,25},ένα υποκατάστατο κρυπτογράφημα ορίζεται από τη συνάρτηση κρυπτογράφησης E_ρ (x) = p (x) και αποκρυπτογράφησης D_p (y) = p^{-1} (x) ,όπου ρ^{-1} είναι η αντίθετη μετάθεση του ρ.

5.1.1 Πρόγνωση κρυπτογραφήματος Καίσαρα

Αυτό το κρυπτογράφημα έχει 26 κλειδιά και μπορεί εύκολα να αποκρυπτογραφηθεί με επίθεση ωμής βίας δοκιμάζοντας και τις 26 αποκρυπτογραφήσεις. Για να αυτοματοποιηθεί η ανάλυση θα ήταν επιθυμητό να βρεθεί η σωστή αποκρυπτογράφηση χωρίς ανθρώπινη παρέμβαση. Επειδή το κλειδί είναι μικρού μήκους, στη συγκεκριμένη περίπτωση μπορούμε να ελέγξουμε όλες τις πιθανές λύσεις , αλλά θα μελετήσουμε μία πιο άμεση, κρυπταναλυτική προσέγγιση υπολογισμού του κλειδιού βασιζόμενη στη συγκεκριμένη συνάρτηση

κρυπτογράφησης. Το κρυπτογράφημα είναι μία αδύναμη μορφή μονοαλφαβητικού κρυπτογραφήματος που διατηρεί τη σχετική σειρά συχνοτήτων των γραμμάτων της αλφάβητου. Αν μετρήσουμε τις συχνότητες χαρακτήρων σε ένα κρυπτογράφημα, το ιστόγραμμα που θα προκύψει είναι μία κυκλική απεικόνιση του ιστογράμματος συχνοτήτων του απλού κειμένου. Μαζί με την επίθεση ωμής βίας, αρκεί να αλλάζουμε το ιστόγραμμα ως να ταιριάξει με το ένα που χαρακτηρίζει τη γλώσσα του απλού κειμένου.

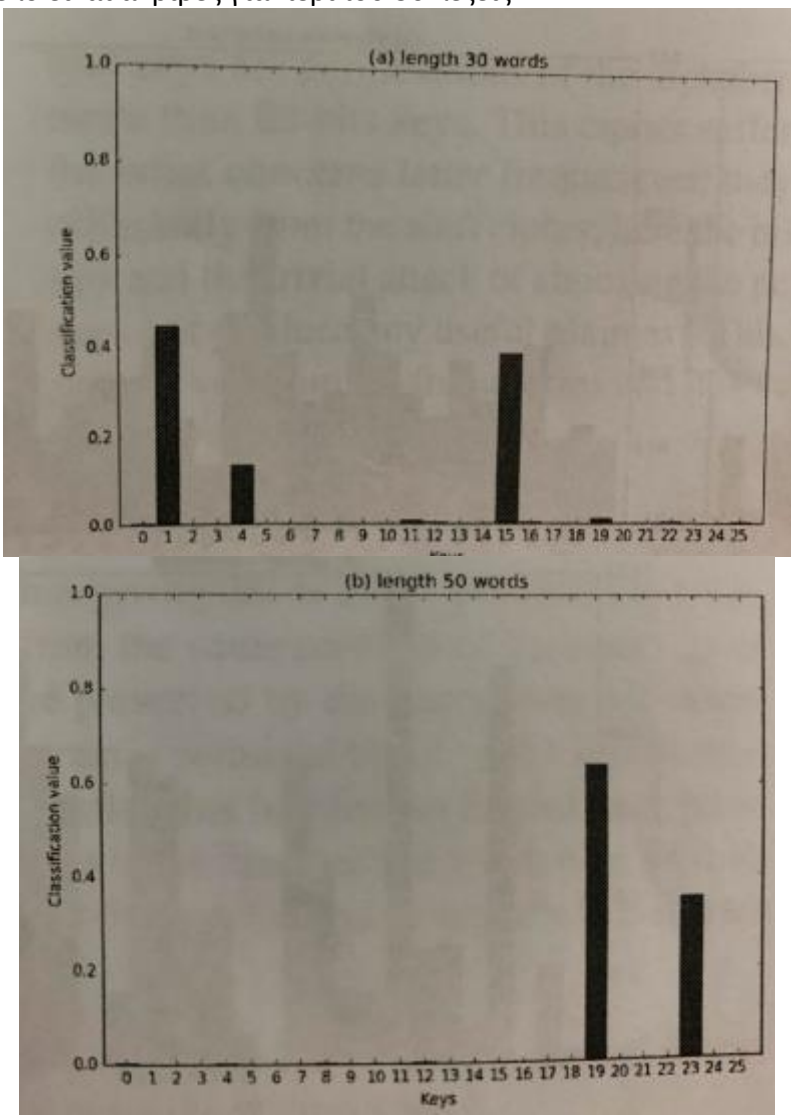


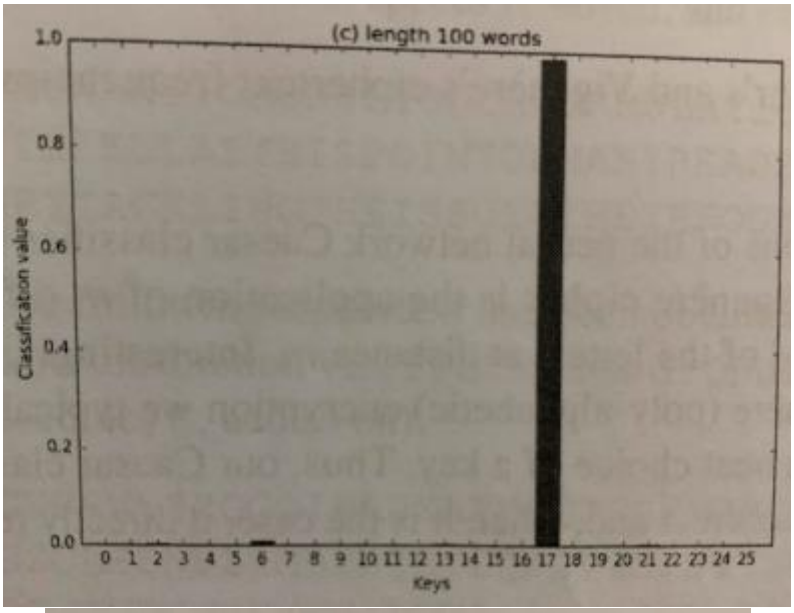
Ένα ΤΝΔ μπορεί να εκπαιδευτεί να αναγνωρίζει την σχετικότητα του ιστογράμματος συχνοτήτων. Το πρόβλημα προσεγγίζεται ως εξής : 1) παίρνουμε ένα αρκετά μεγάλο σύνολο δεδομένων αγγλικών κειμένων που κρυπτογραφήθηκαν 2) υπολογίζουμε τις συχνότητες των γραμμάτων των κρυπτοκειμένων 3) εκπαιδεύουμε ένα ΤΝΔ δίνοντας ως εισροή τις συχνότητες και ως εκροή το κλειδί που ανταποκρίνεται 4)ελέγχουμε το δίκτυο σε ένα ανεξάρτητο σύνολο δεδομένων.

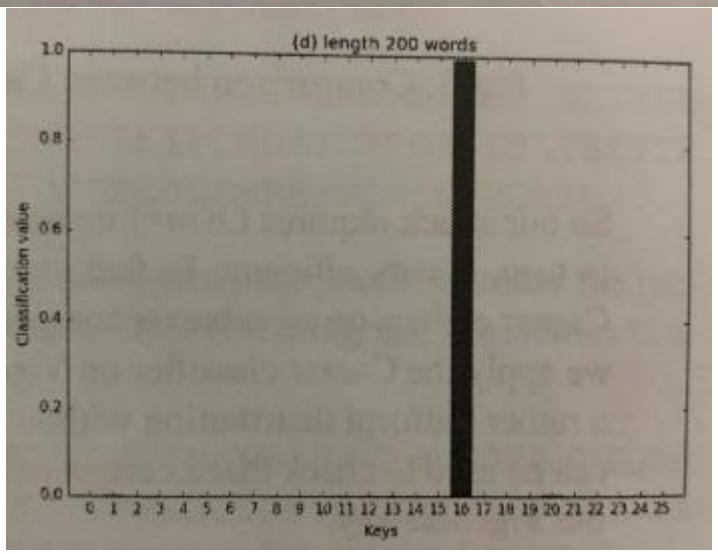
Ο κρυπταναλυτής καταδεικνύει μια αδυναμία και αφήνει στο ΤΝΔ το να τη συνδέσει με το κλειδί κρυπτογράφησης. Το γεγονός ότι το κλειδί υπολογίζεται άμεσα από το ιστόγραμμα δείχνει τη δύναμη των ΤΝΔ για την κρυπτανάλυση του κρυπτογραφήματος.

Αποτελέσματα: Χρησιμοποιούμε ένα ΤΝΔ για ταξινόμηση με επίπεδο εκροής 26 νευρώνων, ένα για κάθε πιθανό κλειδί. Το μόνο κρυμμένο επίπεδο έχει επίσης 26 νευρώνες, δεν

χρειάζεται να γίνει πιο περίπλοκο το δίκτυο. Η συνάρτηση ενεργοποίησης είναι σιγμοειδής σ . Το δίκτυο εκπαιδεύτηκε χρησιμοποιώντας 5097 κρυπτοκείμενα των 100 λέξεων λαμβανόμενα από την κρυπτογράφηση διαφορετικών κειμένων με τυχαία κλειδιά. Δοκιμάσαμε το μοντέλο σε ίδιο αριθμό κρυπτογραφημάτων προερχόμενα από διαφορετικά κείμενα κρυπτογραφημένα με τυχαία κλειδιά και οι δοκιμές είχαν 100% ακρίβεια, επιβεβαιώνοντας ότι το μοντέλο δεν έχει υπερβολικό μέγεθος για τα δεδομένα. Η εκμάθηση διαρκεί περίπου 30 λεπτά και η το σπάσιμο είναι σχεδόν στιγμιαίο. Το μοντέλο είναι ακριβές για περίπου 30 λέξεις.



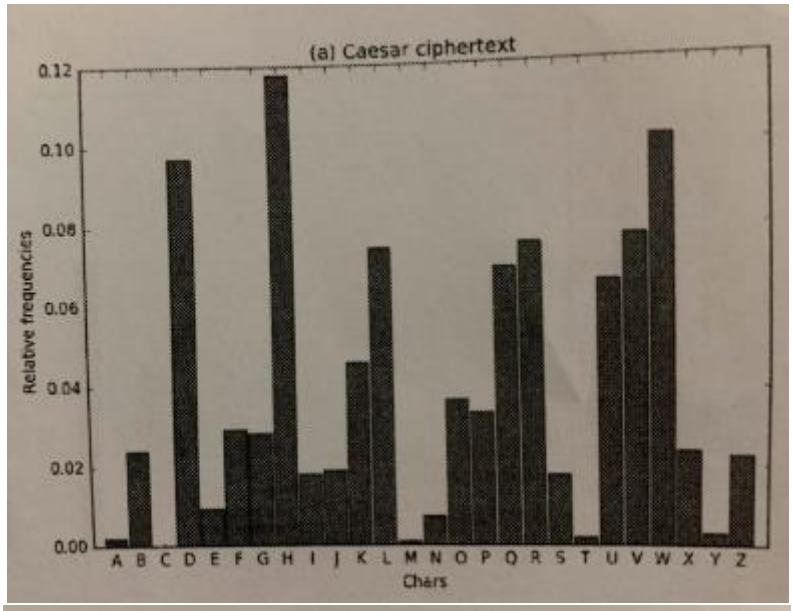


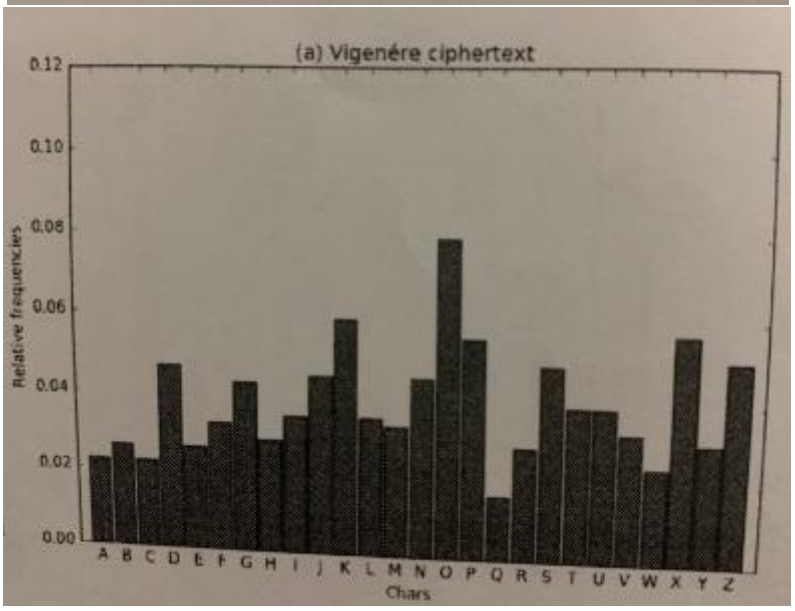


Σε αυτές τις εικόνες φαίνεται η χειρότερη πιθανή τιμή ταξινόμησης για τα επιλεγμένα κλειδιά που προέκυψαν από το ‘’σπάσιμο’’ 5097 κρυπτοκειμένων μήκους 30,50,100 και 200 όπου βρέθηκαν αντίστοιχα τα κλειδιά 1,19,17 και 16. Επιλέγεται το κλειδί με το μεγαλύτερο σκορ. Για μήκος 30, η πρώτη με τη δεύτερη επιλογή είναι κοντά, ενώ για μεγαλύτερα κείμενα η πρόγνωση είναι ξεκάθαρη. Αυτό συμβαίνει γιατί σε μικρές προτάσεις οι σχετικές συχνότητες διαφέρουν περισσότερο από τις μέσες στα Αγγλικά.

5.1.2 ‘’Σπάζοντας’’ το κώδικα Vigenere

Το κρυπτογράφημα Vigenere είναι ένα πολύ-αλφαβητικό κρυπτογράφημα. Βλέπουμε το ιστόγραμμα του συγκρινόμενο με αυτό ενός μονοαλφαβητικού κρυπτογραφήματος και παρατηρούμε ότι έχει ένα πιο ομοιόμορφο σχήμα, το οποίο οφείλεται ακριβώς στο ότι είναι πολύ-αλφαβητικό.





Ένα κρυπτογράφημα Vigenere προσθέτει ένα κωδικό μήκους m σε κάθε μπλοκ απλού κειμένου μήκους m. Η ιδέα είναι να χρησιμοποιηθούν στατιστικά μέτρα σύμπτωσης όπως το Index of Coincidence (IC) για τον έλεγχο αν κάποιο δευτερεύον κείμενο του κρυπτογραφήματος μοιάζει με Αγγλικά σε όρους συχνοτήτων. IC είναι η πιθανότητα ότι δύο τυχαία επιλεγμένα γράμματα είναι ίσα και υπολογίζεται ως το άθροισμα των τετραγώνων των πιθανοτήτων των γραμμάτων. Διατηρείται από μονοαλφαβητικούς μετασχηματισμούς. Για να εντοπιστεί αν το m αρκεί να δοκιμαστούν όλα τα πιθανά μήκη κλειδιών και να υπολογιστεί το IC του δευτερεύοντος κειμένου που αποτελείται από γράμματα σε απόσταση m στο κείμενο. Μόλις βρεθεί το m, Friedman υιοθέτησε μία μορφή IC την Mutual Index of Coincidence (MIC) για να εντοπίσει τη σχέση μεταξύ των διαφορετικών γραμμάτων του κωδικού. Η κρυπτανάλυση του Friedman είναι πολύ αποτελεσματική. Η επίθεση ωμής βίας του κλειδιού μήκους m επαναλαμβάνοντας έναν αποτελεσματικό υπολογισμό m φορές είναι μια χαρά αρκεί η κρυπτογράφηση και η αποκρυπτογράφηση να έχει πολυώνυμο πολυπλοκότητας m.

Η επίθεση είναι ως εξής : Έστω $C= c_{0,\ldots,} c_{n-1}$ είναι το Vigenere κρυπτογράφημα που θέλουμε να ΄΄σπάσουμε΄΄ και MAX το μέγιστο μήκος κλειδιού που θέλει να δοκιμάσει ο επιτεθείς. Τότε :

Για κάθε ακέραιο m στο [1,MAX] :

1. Υπολογίζω όλα τα m δευτερεύοντα κείμενα S_i του C που αποτελείται από γράμματα σε απόσταση m. Πχ, c_0, c_m , c_{m+1} ,..
2. Εφαρμόζουμε Caesar ταξινομητή σε όλα τα S_i ‘ s.
3. Αν ο ταξινομητής επιστρέψει μία τιμή μεγαλύτερη από το κατώφλι t για όλα τα S_i ‘s , η εκροή είναι το κλειδί που βρέθηκε.

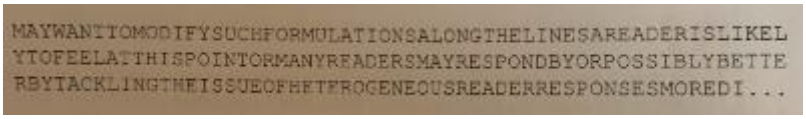
Η πολυπλοκότητα της επίθεσης είναι O (MAX^2) και μπορεί να σπάσει ένα κρυπτογράφημα άμεσα.

Αποτελέσματα: Η επίθεση δοκιμάστηκε σε κείμενα μήκους 400 και 1000 λέξεων με κατώφλια 0,95 και 0,98 αντίστοιχα. Τα κλειδιά επιλέχθηκαν τυχαία με μήκος 5 ως 8. Για τα κείμενα των 400 λέξεων, το ποσοστό λάθος κλειδιών ήταν περίπου 1%. Συνήθως όταν το κλειδί αποτελείται από παρόμοια γράμματα, βρίσκεται λάθος κλειδί, αλλά ακόμη και έτσι όταν παράγονται λάθος κλειδιά, ως εκροή δίνεται και το σωστό. Για κείμενα 1000 λέξεων η επίθεση είναι πολύ ακριβής και δεν ανακτήθηκαν λάθος κλειδιά.

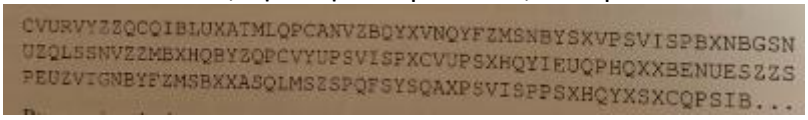
5.1.3 Νευρική κρυπτανάλυση υποκατάστατου κρυπτογραφήματος

Αυτό το κρυπτογράφημα αποτελεί πρόκληση λόγω του υπερβολικά μεγάλου χώρου πιθανών κλειδιών. Τα κλειδιά είναι παραλλαγές του αλφάβητου με πιθανά κλειδιά 26!≈ $2^{88.38}$. Εδώ το ιστόγραμμα βασίζεται στο υποκατάστατο κλειδί και η επίθεση που ταιριάζει περισσότερο στο αγγλικό ιστόγραμμα δεν παράγει χρήσιμο απλό κείμενο. Αυτό συμβαίνει γιατί πολλά αγγλικά γράμματα έχουν παρόμοιες συχνότητες και όταν τα κείμενα είναι μικρά, ανταλλάσσονται.

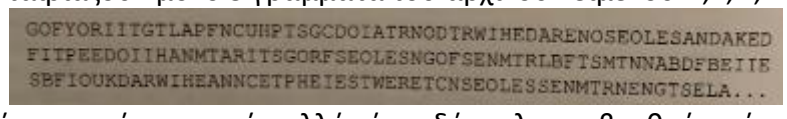
Παράδειγμα 1: Παίρνουμε το παρακάτω κείμενο 200 λέξεων, χωρίς κενά και κομμένα σε τρείς γραμμές



Κρυπτογραφούμε το κείμενο με τη τυχαία υποκατάσταση VETISLFMBDGNCYQHJPXZAORKUW ,δηλαδή το A γίνεται V, το B γίνεται E κλπ. :



Αν χρησιμοποιήσουμε τη μέθοδο συχνοτήτων παίρνουμε το εξής μη επιθυμητό αποτέλεσμα, όπου ταιριάζουν μόνο 5 γράμματα του αρχικού κειμένου B,E,H,K και V.



Αυτή η περίπτωση είναι ατυχής αλλά είναι δύσκολο να βρεθούν πάνω από 10-11 σωστά γράμματα από τα 26 με αυτή τη μέθοδο.

Όταν ψάχνουμε για σειρές n γραμμάτων,n-gram, είναι πιθανό να έχουμε πιο ακριβές μοντέλο μιας γλώσσας. Ωστόσο, επειδή κάθε γράμμα αντικαθίσταται από ένα διαφορετικό ανεξαρτήτων των άλλων, δεν υπάρχει άμεση μέθοδος να χρησιμοποιηθούν n-gram συχνότητες και να βρεθεί πιθανό κλειδί, όπως το παράδειγμα με τα μόνα γράμματα.
Τα n-grams χρησιμοποιούνται για να ορίσουν μία συνάρτηση που δηλώνει πόσο καλό είναι ένα δοθέν κλειδί και επιτρέπει να ψάχνουμε για καλύτερο με τυχαίες σαρώσεις. Η διαδικασία έχει ως εξής:

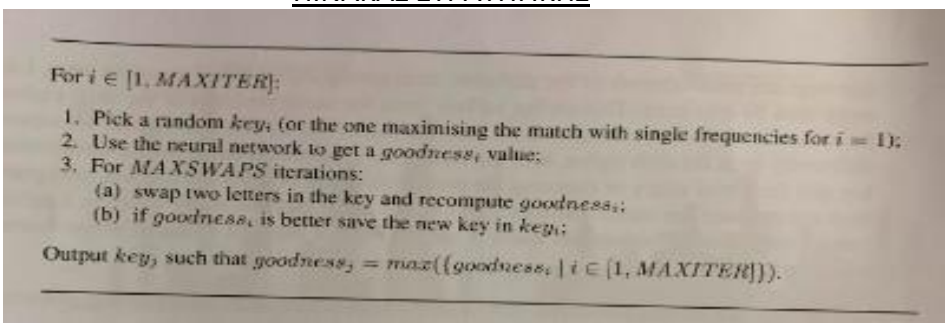
1. Παίρνουμε ένα μεγάλο σύνολο δεδομένων αγγλικών κειμένων που κρυπτογραφήθηκαν με τυχαία κλειδιά.

2. Υπολογίζουμε τις συχνότητες 3-grams των κειμένων και των κρυπτοκειμένων.
3. Εκπαιδεύουμε ένα ΤΝΔ δίνοντας ως εισροή τις συχνότητες και ένα bit εκροής : 1 όταν η εισροή είναι απλό κείμενο,0 όταν είναι κρυπτογραφημένο.
4. Δοκιμάζουμε το ΤΝΔ σε ένα ανεξάρτητο σύνολο δεδομένων.

ΑΠΟΤΕΛΕΣΜΑΤΑ: Το ΤΝΔ έχει ένα κρυμμένο επίπεδο 676 νευρώνων και ένα μονό νευρώνα ως εκροή, δίνοντας τιμή στο φάσμα [0,1]. Τα πειράματα έδειξαν ότι μεγαλώνοντας το μέγεθος, καθυστερεί η εκπαίδευση χωρίς να επιτυγχάνεται ακρίβεια.

Η στρατηγική της επίθεσης επιλέγει ένα τυχαίο κλειδί, αποκρυπτογραφεί το κρυπτογράφημα και χρησιμοποιεί το ΤΝΔ για να εκτιμήσει πόσο σχετικό είναι το κείμενο με τα αγγλικά και το κείμενο-στόχος. Τότε αλλάζει τυχαία γράμματα ψάχνοντας για καλύτερο κείμενο. Αν το ΤΝΔ δίνει καλύτερο αποτέλεσμα, κρατάμε το νέο κλειδί, αλλιώς δοκιμάζουμε νέα τυχαία αλλαγή. Ο επιτεθείς μπορεί να επιλέξει το όριο MAXSWAPS , που είναι ο μέγιστος αριθμός των πιθανών αλλαγών.

ΠΙΝΑΚΑΣ ΣΤΡΑΤΗΓΙΚΗΣ

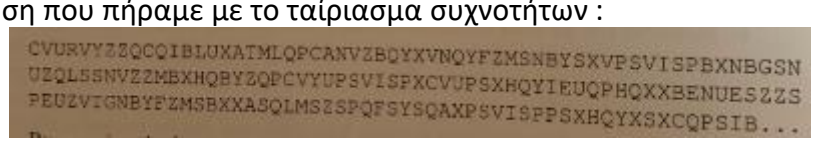


For $i \in [1, MAXITER]$:

1. Pick a random key_i (or the one maximising the match with single frequencies for $i = 1$);
2. Use the neural network to get a $goodness_i$ value;
3. For $MAXSWAPS$ iterations:
   (a) swap two letters in the key and recompute $goodness_i$;
   (b) if $goodness_i$ is better save the new key in key_i;

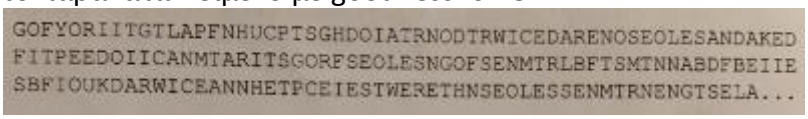
Output key_j such that $goodness_j = max(\{goodness_i \mid i \in [1, MAXITER]\})$.

Παράδειγμα 2: Έχουμε το κρυπτογράφημα του παραδείγματος 1.Ξεκινάμε με την αποκρυπτογράφηση που πήραμε με το ταίριασμα συχνοτήτων :



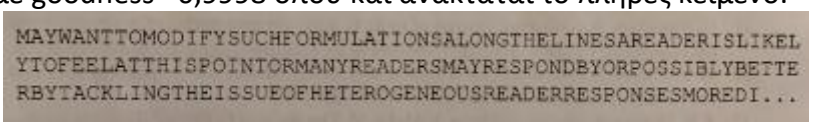
```
CVURVYZZQCQIBLUXATMLQPCANVZBQYXVNQYFZMSNBYSXVPSVISPBXNBGSN
UZQL5SNVZ2MBXHQBYZQPCVYUPSVISPXCVUPSXHQYIEUQPHQXXBENUES2ZS
PEUZVIGNBYFZMSBXXASQLMSZSPQFSYSQAXPSVISPPSXHQYXSXCQPSIB...
```

Το ΤΝΔ παρέχει μία *goodness* αξία περίπου 0,38, επιβεβαιώνοντας ότι το κείμενο απέχει από το να είναι αγγλική πρόταση. Η στρατηγική επίθεσης επιλέγει τυχαία να αλλάξει το γράμμα C με το H , δίνοντας το παρακάτω κείμενο με goodness=0.78.



```
GOFYORIITGTLAPFNHUCPTSGHDOIATRNODTRWICEDARENOSEOLESANDAKED
FITPEEDOIICANMTARITSGORFSEOLESNGOFSENMTRLBFTSMTNNABDFBEIIE
SBFIOUKDARWICEANNHETPCEIESTWERETHNSEOLESSENMTRNENGTSELA...
```

Εφόσον η goodness βελτιώνεται κρατάμε το νέο κλειδί και η διαδικασία συνεχίζεται με το επόμενο κείμενο με goodness =0,9998 όπου και ανακτάται το πλήρες κείμενο:



```
MAYWANTTOMODIFYSUCHFORMULATIONSALONGTHELINESAREADERISLIKEL
YTOFEELATTHISPOINTORMANYREADERSMAYRESPONDBYORPOSSIBLYBETTE
RBYTACKLINGTHEISSUEOFHETEROGENEOUSREADERRESPONSESMOREDI...
```

Δοκιμάσαμε τη τεχνική σε 2500 κείμενα 200 λέξεων. Στο 58% των περιπτώσεων, ανακτήθηκε πλήρως το κλειδί. Στο 93% των περιπτώσεων, το κλειδί έχει το μέγιστο 2 λάθος εκτιμήσεις, όπου το κλειδί βρέθηκε με χειροκίνητη επιθεώρηση. Στο 70% των περιπτώσεων, το καλύτερο κλειδί βρέθηκε με την πρώτη. Οι επιθέσεις έγιναν με MAXITER=10 και MAXSWAPS= 400 και κρατάει 30 δευτερόλεπτα για κάθε κρυπτογράφημα. Ωστόσο , εφόσον στο 70% των

περιπτώσεων το κλειδί βρέθηκε με την πρώτη, η επίθεση διαρκεί 3 δευτερόλεπτα ως να βρεθεί το κλειδί.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Σε αυτό το κεφάλαιο, παρουσιάστηκε το πως μπορούμε να χρησιμοποιήσουμε τις υπάρχουσες τεχνικές κρυπτανάλυσης για τα κλασσικά κρυπτογραφήματα με τα ΤΝΔ που μπορούν να αυτοματοποιήσουν μέρος της επίθεσης. Αναδείξαμε πως τα ΤΝΔ επιτρέπουν στον κρυπταναλυτή να εστιάσει στα ενδιαφέροντα χαρακτηριστικά των αδυναμιών του κρυπτογραφήματος, και τα δίκτυα τα συνδυάζουν και παράγουν είτε το κλειδί ή την *goodness* του κλειδιού που ανακτήθηκε με επίθεση ωμής βίας.

5.2 Τεχνητά Νευρωνικά Δίκτυα για Κρυπτογραφικά Προβλήματα

Σε αυτή την ενότητα, θα μελετηθεί η συμπεριφορά των Νευρωνικών Δικτύων σε κάποια κρυπτογραφικά προβλήματα. Συγκεκριμένα, θα μελετηθεί η προσέγγιση του Διακριτού Προβλήματος Λογαρίθμου/ Discrete Logarithm Problem (DLP) και το πρόβλημα ανταλλαγής κλειδιού του πρωτόκολλου Diffie- Hellman / Diffie –Hellman key-exchange protocol problem (DHP) στο ορισμένο πεδίο Z ,όπου p είναι πρώτος αριθμός και το πρόβλημα παραγοντοποίησης συνδέεται με το κρυπτοσύστημα RSA.

5.2.1 Παρουσίαση πειράματος και αποτελέσματα.

Αλγόριθμοι : Σε αυτή τη μελέτη, οι αλγόριθμοι ΤΝΔ που υπολογίστηκαν, είναι Standard Back Propagation (BP) , Back Propagation with Variable Stepsize (BPVS), Resilient Back Propagation (RPROP), On- Line Adaptive Back Propagation (OABP) και η Scaled Conjugate Gradient method (SCG). Όλες οι μέθοδοι δοκιμάστηκαν σε ένα μεγάλο εύρος παραμέτρων. Στις πιο πολλές περιπτώσεις, δεν υπήρχαν σημαντικές διαφορές μεταξύ τους στην απόδοση, εκτός από την BP, που παρουσίασε δυσκολίες τις περισσότερες φορές.

Αρχιτεκτονική δικτύου: Η έννοια της ‘’βέλτιστης’’ αρχιτεκτονικής δικτύου για οποιοδήποτε πρόβλημα είναι δύσκολη και παραμένει ανοιχτό πρόβλημα, δοκιμάσαμε ποικιλία τοπολογιών με διαφορετικό αριθμό κρυμμένων στρωμάτων και ποικιλία στον αριθμό των νευρών σε κάθε επίπεδο. Τα αποτελέσματα που αναφέρονται, είναι τα καλύτερα για κάθε πρόβλημα. Η αρχιτεκτονική που χρησιμοποιήθηκε περιγράφεται με μία σειρά ακεραίων αριθμών που δηλώνουν τον αριθμό των νεύρων σε κάθε στρώμα.

Ομαλοποίηση δεδομένων : Για να γίνει η αποδοχή του δικτύου ευκολότερη, τα δεδομένα μετατρέπονται μέσω της διαδικασίας ομαλοποίησης, που γίνεται πριν τη δοκιμή. Υποθέτουμε ότι τα δεδομένα που παρουσιάζονται στο δίκτυο, ανήκουν στο Z_p , όπου p είναι πρώτος αριθμός, και ο χώρος S= [-1,1] , χωρίζεται σε p υποσύνολα. Τα νούμερα στο σύνολο των δεδομένων μετατρέπονται σε ανάλογα στον χώρο S. Την ίδια στιγμή, η εκροή του δικτύου μετατρέπεται σε έναν αριθμό μέσα στο Z_p χρησιμοποιώντας την αντίστροφη διαδικασία.

Αξιολόγηση Δικτύου : Για την αξιολόγηση της απόδοσης του δικτύου μετράμε πρώτα το ποσοστό των δεδομένων που θα χρησιμοποιηθούν, για τα οποία το δίκτυο μπορεί να υπολογίσει την ακριβή αξία στόχου. Αυτή η μέτρηση εκφράζεται με μ_0 . Ωστόσο, όσο η εκροή του δικτύου έχει περιοριστεί στο εύρος [-1,1] , πολύ μικρές διαφορές στις εκροές, αποδίδονται να κάνουν το δίκτυο ανίκανο να υπολογίσει τον σωστό στόχο, αλλά να είναι πολύ κοντά σε αυτό. Αυτό συνέβη

λόγω της αναποτελεσματικότητας του μέτρου μ_0 ως ενδείκτη απόδοσης. Για αυτό χρησιμοποιούμε τον δείκτη $\mu_{+-\upsilon}$. Αυτός ο μετρητής αναπαριστά το ποσοστό των δεδομένων για τα οποία η διαφορά μεταξύ επιθυμητής και πραγματικής εκροής δε ξεπερνά ± υ του πραγματικού στόχου.

Το μέτρο , $\mu_{\pm\upsilon}$, έχει διαφορετικό νόημα για τον DLP και για το DHP . Το $\mu_{\pm\upsilon}$ είναι πολύ σημαντικό για την περίπτωση DLP. Αν μέγεθος του (±υ) διαστήματος είναι O (log(p)), τότε το ‘’περίπου’’ μέτρο μπορεί να αντικαταστήσει το ακριβές μ_0 . Γενικά, για μικρές αξίες του υ είναι αποδεκτό το ‘’κοντινό’’ μέτρο εφόσον ο υπολογισμός του διακριτού λογάριθμου μπορεί να πιστοποιηθεί. Ωστόσο η επιβεβαίωση της ελλειπτικής καμπύλης Diffie- Hellman είναι ένα ανοιχτό πρόβλημα. Σύνολα πιθανών τιμών για την ελλειπτική καμπύλη Diffie- Hellman μπορούν να χρησιμοποιηθούν για τον υπολογισμό συνόλων πιθανών τιμών για το κλειδί Diffie- Hellman. Οι τιμές κλειδιού Diffie- Hellman μπορούν να δοκιμαστούν στην πράξη, είναι συμμετρικά κλειδιά επικοινωνίας μεταξύ δύο χρηστών. Το ποσοστό επιτυχίας του ‘’κοντινού’’ μέτρου για DHMP μπορεί να συγκριθεί με το αντίστοιχο ποσοστό DLP. Τα αποτελέσματα της σύγκρισης μπορούν να συσχετιστούν με την υπόθεση ότι τα δύο προβλήματα είναι υπολογιστικά ισάξια.

Εξετάστηκαν πολλές τιμές μικρών πρώτων αριθμών p. Οι εισροές προτύπων ήταν διαφορετικές τιμές από την τιμή εισροής της συνάρτησης του διακριτού λογάριθμου και της καμπύλης Diffie- Hellman, και τα πρότυπα στόχου ήταν οι τιμές της αντίστοιχης συνάρτησης, για προκαθορισμένες επιλεγμένες τιμές των γεννητριών g και των πρώτων p. Τα ΤΝΔ σε αυτή την περίπτωση πέτυχαν στις δοκιμές και στις γενικεύσεις, φτάνοντας το 100%. Μετά, δοκιμάστηκαν μεγαλύτεροι πρώτοι αριθμοί για να δοκιμάσουν σκληρότερα τα δίκτυα. Έχοντας τόσους πολλούς αριθμούς να κανονικοποιούνται στο εύρος [-1,1] δημιουργήθηκαν προβλήματα στην διαδικασία. Έτσι, μικρές αλλαγές στην εκροή του δικτύου προκάλεσε ολοκληρωτική καταστροφή, απαιτώντας τη χρήση μεγαλύτερων αρχιτεκτονικών, πχ κόμβων και στρωμάτων. Στις περιπτώσεις μεγάλων πρώτων, η απόδοση δικτύου ήταν πολύ φτωχή.

Αποτελέσματα με DLP και DHMP.

p	Topology	Epochs	μ_0	$\mu_{\pm 2}$	$\mu_{\pm 5}$	$\mu_{\pm 10}$	Problem
83	$1-5-5-1$	20000	20%	30%	48%	70%	DLP
	$1-5-5-1$	20000	20%	35%	51%	70%	DHMP
97	$1-5-5-1$	25000	20%	30%	48%	70%	DLP
	$1-5-5-1$	20000	20%	35%	51%	70%	DHMP

Ο DLP μελετήθηκε για διάφορες τιμές του πρώτου p και της αρχικής ρίζας g, η αξία $h=g^u$ (modp), παραμένει σταθερή. Τα πρότυπα εισροής αποτελούνται από ζευγάρια πρώτων p και τις αντίστοιχες ρίζες g και τα πρότυπα στόχου ήταν οι αντίστοιχες αξίες του u, τέτοιες ώστε $\log_g h \equiv u$ (mod p) , για μία επιλεγμένη προκαθορισμένη τιμή h. Δοκιμές έγιναν για τιμές p μεταξύ 101 και 2003, με ποικίλες τοπολογίες δικτύου και μεθόδους. Σε αυτή τη περίπτωση, υπάρχει διαφοροποίηση ανάμεσα στα αποτελέσματα που πάρθηκαν από διαφορετικές μεθόδους. Για παράδειγμα, για μικρές τιμές p, από 101-199, τα καλύτερα αποτελέσματα τα δίνει η μέθοδος AOBP, για μεγαλύτερες τιμές του p, η SCG.
Όλα τα αποτελέσματα αναφέρονται στην εκπαίδευση των ΤΝΔ στην προσέγγιση της τιμής του διακριτού λογάριθμου u. Φαίνεται ότι για το πρόβλημα DLP , τα FNNs είναι καλύτερα.

Αποτελέσματα για την $2^{η}$ ρύθμιση του DLP.

Range of p	Topology	Epochs	μ_0	$\mu_{\pm 15}$	$\mu_{\pm 20}$	$\mu_{\pm 30}$	$\mu_{\pm 40}$
$101 - 199$	$2 - 15 - 1$	600000	100%	100%	100%	100%	100%
$503 - 1009$	$2 - 25 - 1$	600000	82%	93%	96%	96%	98%
$1009 - 2003$	$2 - 30 - 1$	600000	17%	40%	46.7%	51.8%	54.1%
$1009 - 2003$	$2 - 3 - 3 - 3 - 1$	20000	7.5%	34.3%	44.8%	64.2%	71.6%

Μελετήθηκε η ικανότητα των νευρωνικών δικτύων να ανταποκριθούν σε RSA κρυπτοσυστήματα. Στον πίνακα φαίνονται τα αποτελέσματα για δίκτυα που δοκιμάστηκαν για ø (N) σχεδιασμό , N →ø (N), με εισροή N=p x q , όπου p και q είναι πρώτοι και τα μοτίβα στόχου ø (N) = (p-1) x (q-1) αριθμοί. Τα δίκτυα ανταποκρίθηκαν και είχαν πολύ καλά αποτελέσματα.

Αποτελέσματα για σχεδιασμό ø (N) με N= p x q ≤ 10^{4}

Topology	Epochs	μ_0	$\mu_{\pm 2}$	$\mu_{\pm 5}$	$\mu_{\pm 10}$	$\mu_{\pm 20}$
$1 - 5 - 5 - 1$	80000	3%	15%	35%	65%	90%
$1 - 7 - 8 - 1$	50000	6%	20%	50%	70%	100%

Το πρόβλημα παραγοντοποίησης μελετήθηκε σε διαφορετική σύνθεση. Συγκεκριμένα, προσεγγίζοντας την τιμή της συνάρτησης $p^2 + q^2$, δοσμένης της αξίας του N, οδηγεί κατευθείαν στην παραγοντοποίηση του N στους παράγοντες του p και q. Μελετήθηκαν τα ANNs για την προσέγγιση της συνάρτησης για διάφορες τιμές του N.

Αποτελέσματα για τη δεύτερη ρύθμιση του προβλήματος παραγοντοποίησης για το N με εύρος 143-1003.

Topology	Epochs	μ_0	$\mu_{\pm 15}$	$\mu_{\pm 20}$	$\mu_{\pm 30}$	$\mu_{\pm 40}$
$1 - 15 - 1$	200000	35.1%	36.8%	42.1%	43.8%	45.6%
$1 - 20 - 1$	600000	35.1%	43.8%	45.6%	52.6%	56.2%

Οι δύο εκδοχές του προβλήματος παραγοντοποίησης είναι υπολογιστικά ισάξια για τα FNNs φαίνεται να ναι καλύτερο για την πρώτη. Αν μία μέθοδος υπολογισμού δεικτών για ορισμένο πεδίο είναι διαθέσιμο, τότε το RSA κρυπτοσύστημα. Το DLP δεν είναι ευκολότερο από το πρόβλημα παραγοντοποίησης σχετισμένο με το RSA, που επιβεβαιώνεται από την έρευνα.

5.2.2 Τεχνητά Νευρωνικά Δίκτυα Σε προβλήματα σχετικά με την Κρυπτογραφία Ελλειπτικής Καμπύλης

Εδώ θα μελετηθεί η απόδοση των ΤΝΔ στο πρόβλημα υπολογισμού του τελευταίου σημαντικού bit του διακριτού λογαρίθμου σε ένα σημείο καμπύλης ελλειπτικής καμπύλης. Ο υπολογισμός αυτού του bit σε ελλειπτικές καμπύλες με τις γνωστές περίεργες σειρές είναι σημαντικός γιατί θα οδηγήσει στον υπολογισμό όλων των bit του διακριτού λογαρίθμου. Τα αποτελέσματα της χρήσης ANNs για τέτοια προβλήματα, δείξαν στην πρώτη προσπάθεια ότι τα ANNs μπορούν να προσαρμοστούν στα δεδομένα με ακρίβεια, ενώ η απόκριση τους σε άγνωστα δεδομένα είναι υψηλότερη από την τυχαία επιλογή. Επίσης τα ANNs απαιτούν λιγότερο χώρο αποθήκευσης για τα γνωστά πρότυπα, σε αντίθεση με τον χώρο για τα δεδομένα καθαυτά.

Μορφοποίηση Προβλήματος

Πρόταση 1

Δοθείσας μίας ελλειπτικής καμπύλης ,E, σε ένα ορισμένο πεδίο F_q , με γνωστή σειρά n και μία εικασία για ένα bit του διακριτού λογαρίθμου που δεν ανταποκρίνεται σε καμία δύναμη των 2 που χωρίζουν τη σειρά n , τότε όλα τα bits του διακριτού λογαρίθμου μπορούν να υπολογιστούν σε πολυωνυμικό χρόνο.

Σημ. : Δεν υπάρχει πολυωνυμικός αλγόριθμος για να βρεθεί η σειρά της ελλειπτικής καμπύλης. Ωστόσο η πολυπλοκότητα υπολογισμού του προβλήματος διακριτού λογαρίθμου σε ελλειπτικές καμπύλες χωρίς γνώση της σειράς που είναι εκθετική και παραμένει υπολογιστικά πολύ δύσκολο έργο.

Από την πρόταση, προκύπτει ότι στην περίπτωση της ελλειπτικής τροχιάς με άστατη σειρά n, μια εικασία που δίνει το ελάχιστα σημαντικό bit του διακριτού λογάριθμου ενός σημείου της ελλειπτικής τροχιάς οδηγεί στον υπολογισμό όλων των bits του διακριτού λογάριθμου. Ωστόσο, πιο ασφαλής θεωρούνται οι ελλειπτικές καμπύλες πρώτης τάξης.
Χρησιμοποιούμε συνάρτηση Boolean ως εξής : Έστω μία ελλειπτική τροχιά $E(F_p)$ και $P=(x_p , y_p)$,$Q= (x_Q, y_Q)$ είναι δύο σημεία της $E(F_p)$, τέτοια ώστε $Q= Tp$, με $0\leq t \leq (n-1)$. Ορίζουμε την συνάρτηση Boolean $f : \{ 0,1\}^{4[logp]} \rightarrow \{0,1 \}$ με
$f (x_P, y_P, x_Q ,y_Q) = lsb(t)$
με εισροές τις συντεταγμένες x_P, y_P, x_Q ,y_Q , σε δυαδική αναπαράσταση και εκροές το λιγότερο σημαντικό bit του t, π.χ. 1 αν το λιγότερο σημαντικό bit του t είναι 1, 0 για το αντίστροφο.

Χρησιμοποιούμε ΤΝΔ για τον υπολογισμό αυτής της συνάρτησης που προκύπτει από την κρυπτογραφία ελλειπτικής τροχιάς.

Θεώρημα : Υπάρχει ένα δίκτυο κατωφλίου με ένα κρυμμένο επίπεδο ικανό να υπολογίσει οποιαδήποτε συνάρτηση Boolean.

Ρύθμιση πειράματος και αποτελέσματα.

Τα αναλογικά ΝΔ μπορούν να είναι πιο δυνατά από τα ΝΔ που χρησιμοποιούν κατώφλια, ακόμη και για τον υπολογισμό συναρτήσεων Boolean. Μελετάμε την απόδοση των ΤΝΔ χρησιμοποιώντας τη συνάρτηση ενεργοποίησης υπερβολικής εφαπτομένης, που προσεγγίζει μία συνάρτηση κατωφλίου όσο το λ_2 τείνει στο άπειρο. Σε όλα τα πειράματα, το εξωτερικό στρώμα αποτελείται από δύο νευρώνες και ο νευρώνας με την μεγαλύτερη αξία εκροής ορίζει την κλάση στην οποία θα ταξινομηθεί το υπολογισμένο bit. Έτσι, αν η τιμή της εκροής του πρώτου νευρώνα είναι μικρότερη από αυτή του δεύτερου, το bit ανήκει στην κλάση 0, που μεταφράζεται σε ‘’0’’ τιμή του bit, και το αντίστροφο.

Χρησιμοποιήθηκαν τρείς αλγόριθμοι ο καθένας από διαφορετική κατηγορία, τους : Resilient Back Propagation method (RPROP), Adaptive On-line Back Propagation method (AOBP), και Differential Evolution Algorithm (DE). Δοκιμάστηκαν διαφορετικές τοπολογίες και αριθμοί νευρώνων σε κάθε στρώμα και παρουσιάζονται τα καλύτερα αποτελέσματα.

Σε κάθε πείραμα, τα σύνολα δεδομένων, τυχαία συμμετείχαν σε σύνολα εκπαίδευσης και σε σύνολα τεστ. Τα δύο τρίτα του συνόλου δεδομένων αποδόθηκαν σε σύνολο εκπαίδευσης δεδομένων και τα υπόλοιπα συμπλήρωσαν το σύνολο τεστ. Για να αξιολογηθεί η απόδοση δικτύου, πρώτα μετράμε το μέσο όρο του ποσοστού των δοκιμών σε 10 πειράματα, για τα οποία

το δίκτυο ήταν ικανό να μαντέψει σωστά το λιγότερο σημαντικό ψηφίο. Έπειτα, υπολογίζεται η απόδοση δικτύου μετρώντας το μέσο ποσοστό του συνόλου σε όλα τα πειράματα.

Συμπεράσματα

Βλέπουμε τα καλύτερα αποτελέσματα στους παρακάτω πίνακες όπου $\lambda_2 = 1$, με την AOBP μέθοδο. Για τρία μήκη bit, τα ΤΝΔ μπόρεσαν να προσαρμοστούν με ποσοστό 90%. Όσο αυξάνεται το μήκος του ρ, χρειάζονται περισσότερες επαναλήψεις για την ίδια αποτελεσματικότητα.

Αποτέλεσμα για ρ με μήκος bit 14, και τοπολογία 56-3-2

Epochs		Train			Test		
		Class 0	Class 1	Accuracy	Class 0	Class 1	Accuracy
500	Class 0	168	33	83.58%	30	24	55.56%
	Class 1	48	151	75.88%	23	23	50.00%
650	Class 0	184	17	91.54%	33	21	61.11%
	Class 1	32	167	83.92%	23	23	50.00%
700	Class 0	183	18	91.04%	33	21	61.11%
	Class 1	30	169	84.92%	21	25	54.35%
1000	Class 0	186	15	92.54%	33	21	61.11%
	Class 1	25	174	87.44%	18	28	60.87%

Αποτέλεσμα για ρ με μήκος bit 20, και τοπολογία 80-3-2

Epochs		Train			Test		
		Class 0	Class 1	Accuracy	Class 0	Class 1	Accuracy
2000	Class 0	186	14	93.0%	32	26	55.17%
	Class 1	23	177	88.5%	17	25	59.52%
3000	Class 0	191	9	95.5%	30	28	51.72%
	Class 1	19	181	90.5%	21	21	50.00%
4000	Class 0	194	6	98.0%	32	26	55.17%
	Class 1	18	182	91.0%	19	23	54.76%
6000	Class 0	196	4	98.0%	33	25	56.90%
	Class 1	17	183	91.5%	20	22	52.38%

Αποτέλεσμα για ρ με μήκος bit 32, και τοπολογία 128-3-2

Epochs		Train			Test		
		Class 0	Class 1	Accuracy	Class 0	Class 1	Accuracy
4000	Class 0	193	5	97.47%	36	21	63.16%
	Class 1	16	186	92.08%	20	23	53.49%
5000	Class 0	193	5	97.47%	36	21	63.16%
	Class 1	15	187	92.57%	19	24	55.81%
8000	Class 0	193	5	97.47%	35	22	61.40%
	Class 1	14	188	93.07%	18	25	58.14%
9000	Class 0	193	5	97.47%	35	22	61.40%
	Class 1	14	188	93.07%	16	27	62.79%

Στον παρακάτω πίνακα βλέπουμε τα αποτελέσματα για την συμπίεση δεδομένων. Το BL(p) δηλώνει το μήκος του p , το Data Storage την αποθήκευση bit που απαιτούνται για το σύνολο δεδομένων , το ANNs stor. Τα αποθηκευμένα bits για τα βάρη δικτύου και η Accuracy στην επιτυχία του δικτύου να εντοπίσει την επιθυμητή αξία και για τις δύο κλάσεις.

BL(p)	Data Stor.	ANN Stor.	Accuracy
14	23200	8400	89.99%
20	32800	11856	94.75%
32	52000	18768	95.27%

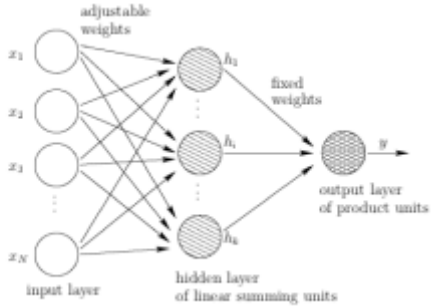
5.3 Πολυωνυμικά Δίκτυα Κορυφογραμμής για Κρυπτογραφία.

Τα Ridge Polynomial Networks (RPNs) ανήκουν στην κλάση των ΤΝΔ που βασίζονται στον παραγωγικό τύπο νευρώνων, οι νευρώνες εκτελούν την συνάρτηση ενεργοποίησης τους στην εκροή των εισροών των βαρών. Τα RPNs έχουν περισσότερα πλεονεκτήματα συγκριτικά με αυτά που έχουν μονάδες άθροισης.

5.3.1 Δίκτυα Pi-Sigma

Τα δομικά στοιχεία των RPNs είναι τα δίκτυα Pi-Sigma. Αυτά τα δίκτυα είναι ένα τροφοδοτικό νευρικό δίκτυο με ένα μόνο ‘’κρυμμένο΄΄ στρώμα γραμμικής μονάδας που παράγει μονάδες σε εξωτερικά στρώματα . Υπάρχουν δύο τύποι τέτοιων δικτύων : τα Analog Pi-Sigma Networks (APSNs), αναλογικά, και τα Binary Pi-Sigma Networks (BPSNs), δυαδικά. Μια πιο ευρεία κατηγορία APSNs είναι τα Ridge Polynomial Networks, τα οποία έχουν γενική ικανότητα, ενώ τα BPSNs είναι ικανά να επιλύσουν οποιαδήποτε συνάρτηση Boolean.

Ένα δίκτυο Pi-Sigma με μία μονάδα εκροής



Αυτό το δίκτυο είναι ένα πλήρως συνδεδεμένο εμπρόσθιο δίκτυο και η μονάδα άθροισης δεν είναι κρυμμένη, γιατί τα βάρη από αυτό το στρώμα προς το εξωτερικό είναι προκαθορισμένα στην τιμή 1. Αυτό βοηθάει στην μείωση του απαιτούμενου χρόνου δοκιμών.

Αν $x=(1,x_1,\ldots..,x_N)^T$ είναι ένα αυξημένο διάνυσμα στήλης εισαγωγής N+1 διαστάσεων, όπου x_k είναι το k-th συστατικό του x. Οι εισροές είναι βαθμονομημένες από K(N+1) διαστάσεων βάρη με διανύσματα $w=(w_{0j} ,w_{1j} ,\ldots, w_{Nj})$, j=1,2,..,K αθροισμένα από ένα στρώμα K γραμμικών μονάδων άθροισης , όπου k είναι η επιθυμητή εντολή του δικτύου. Η εκροή της jth μονάδας, h_j :

$$h_j = \mathbf{w}_j^\top \mathbf{x} = \sum_{k=1}^{N} w_{kj} x_k + w_{0j}, \quad j = 1, 2, \ldots, K.$$

Η εκροή δίνεται :

$$y = \sigma(\prod_{j=1}^{K} h_j) = \sigma(net),$$

Όπου σ(.) είναι η κατάλληλη συνάρτηση ενεργοποίησης και net= $\Pi^{K}_{j=1} h_j$. Το w_{kj} είναι ένα επιπλέον βάρος της εισροής x_k στην jth μονάδα υπολογισμού. Τα βάρη μπορούν να υποθέσουν τυχαίες πραγματικές τιμές.

Το δίκτυο της παραπάνω εικόνας ονομάζεται K-th σειράς PSN επειδή K υπολογιστικές μονάδες συμμετέχουν. Ο συνολικός αριθμός των επιπλέον συνδέσεων βαρών, για ένα K-th PSN με N διαστάσεων εισροές είναι (N+1)K. Αν χρειαστούν πολλαπλές εκροές, χρειάζεται ένα έξτρα ανεξάρτητο υπολογιστικό επίπεδο για κάθε εκροή. Για ένα διάνυσμα εκροής M- διαστάσεων y , ένα σύνολο $\sum_{i=1}^{M}(N+1)K_i$ πρόσθετοι σύνδεσμοι βαρών , όπου $K_ι$ είναι ο αριθμός των υπολογιστικών μονάδων για την ith εκροή. Αυτό επιτρέπει στο δίκτυο να έχει την δυνατότητα επέκτασης, αφού η σειρά μπορεί να αυξηθεί προσθέτοντας υπολογιστική μονάδα και σχετιζόμενα βάρη, χωρίς να επηρεάζεται η προϋπάρχουσα δομή. Τα PSNs μπορούν να χειριστούν αναλογικές και δυαδικές εισροές/εκροές χρησιμοποιώντας την κατάλληλη μη γραμμική συνάρτηση ενεργοποίησης σ(.).

Η συνάρτηση ενεργοποίησης εφαρμόζεται σε ένα K-th πολυώνυμο όταν χρησιμοποιούνται K υπολογιστικές μονάδες και οι εκθέτες i_j αθροίζονται στο K , δεν σημαίνει ότι μόνο K-th σειράς όροι μπορούν να χρησιμοποιηθούν, καθώς βάζοντας μία έξτρα εισροή στην προκαθορισμένη τιμή 1, μπορούν να επεξεργαστούν και τιμές μικρότερες του K. Αυτό το πολυώνυμο δεν έχει πλήρη ανεξαρτησία εφόσον οι συντελεστές είναι σύνθεση των αθροίσεων και των παραγώγων του w_{kj} s και έτσι δεν είναι ανεξάρτητοι. Έτσι ένα PSN δεν μπορεί να προσεγγίσει όλες τις συνεχόμενες πολύπλοκες και παραλλαγμένες συναρτήσεις ενός συνόλου. Ωστόσο η καθολικότητα της ικανότητας των πολυωνύμων κορυφογραμμής επιτυγχάνεται αθροίζοντας τις εκροές των APSNs με διαφορετική σειρά. Το δίκτυο που προκύπτει είναι μία γενίκευση των PSN, που ονομάζεται Ridge Polynomial Network (RPN) (Δίκτυο Πολυωνύμου Κορυφογραμμής) και αναπτύσσεται ως εξής.

Για $x=(x_1,..x_N)^T$ και $w=(w_{1,..},w_N)^T \in R^N$ ορίζουμε ως (x,w) το εσωτερικό τους προϊόν, πχ $[x,w]=\sum_{i=1}^{N} x_i w_i$. Για ένα σύνολο $C \in R^N$, όλες οι οριζόμενες συναρτήσεις στο C της μορφής f((x,w)) , όπου f είναι μία συνεχόμενη σε μία μεταβλητή, και ονομάζονται συναρτήσεις κορυφογραμμής. Ένα πολυώνυμο κορυφογραμμής είναι μία συνάρτηση κορυφογραμμής :

$$\sum_{i=0}^{n}\sum_{j=1}^{m} a_{ij}\langle \mathbf{x}, \mathbf{w}\rangle^i,$$

Για $a_{ij} \in R$ και $w_{ij} \in R^N$

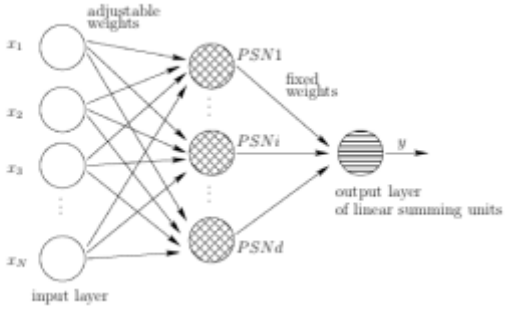
Το πολυωνυμικό δίκτυο κορυφογραμμής ορίζεται ως ένα *feedforward* δίκτυο βασισμένο στην γενική μορφή των δικτύων κορυφογραμμής

$$p(\mathbf{x}) = \sum_{j=1}^{n_{\text{total}}} \prod_{i=1}^{j} (\langle \mathbf{x}, \mathbf{w}_{ji}\rangle + w_{ij}),$$

Όπου $n_{total} = \Sigma^{k}_{l=0} n_l$ και προσεγγίζει μία άγνωστη συνάρτηση f ενός συνόλου $C \subset R^N$ ως εξής :

$$f(\mathbf{x}) \approx (\langle \mathbf{x}, \mathbf{w}_{11}\rangle + w_{11}) + (\langle \mathbf{x}, \mathbf{w}_{21}\rangle + w_{21})(\langle \mathbf{x}, \mathbf{w}_{22}\rangle + w_{22}) + \cdots + (\langle \mathbf{x}, \mathbf{w}_{N1}\rangle + w_{N1}) \cdots (\langle \mathbf{x}, \mathbf{w}_{NN}\rangle + w_{NN}).$$

Ένα πολυωνυμικό δίκτυο κορυφογραμμής (RPN) με μία γραμμική μονάδα εκροής.



Στο σχήμα βλέπουμε την αρχιτεκτονική ενός RPN που χρησιμοποιεί PSNs ως δομικά στοιχεία. Έχει μόνο ένα στρώμα ευπροσάρμοστων βαρών που βοηθούν στην ταχύτητα.

Συμπέρασμα : Η ομοιόμορφη ικανότητα προσέγγισης των RPNs και η ταχύτερη εκπαίδευση τους σε σχέση με άλλα Τεχνητά Νευρωνικά Δίκτυα , τα καθιστά μία υποσχόμενη μεθοδολογία για τα προβλήματα της κρυπτογραφίας.

Σχετικά με τον υπολογισμό του σωστού bit του διακριτού λογαρίθμου από πολυώνυμα , εξάγονται τα εξής θεωρήματα:

Θεώρημα 1 : Έστω $0 \le M < M + H \le p-1$. Υποθέστε ότι ένα πολυώνυμο $f(X) \in R[X]$ είναι τέτοιο ώστε $f(x) \ge 0$ αν x είναι τετραγωνικό κατάλοιπο p και $f(x) < 0$, αλλιώς για κάθε στοιχείο $x \in S$ από σύνολο
$S \subseteq \{ M+1,..,M+H\}$ από $|S| \ge H-s$. Τότε για κάθε $\varepsilon > 0$ το όριο

$$\deg f \geqslant \begin{cases} H/2 - 2s - 1 - p^{1/2}\log p, & for\ any\quad H, \\ \mathcal{C}(\varepsilon)\min\{H, H^2p^{-1/2}\} - 2s - 1, & if\quad p^{1/4+\varepsilon} \leqslant H \leqslant p^{1/2+\varepsilon}, \\ (p-1)/2 - 2s - 1, & if\quad N = 0, H = p-1, \end{cases}$$

holds, where $\mathcal{C}(\varepsilon) > 0$ depends only on ε.

Επίσης, όσο αφορά πολυμερή πολυώνυμα , εξάγεται το ακόλουθο θεώρημα :

Θεώρημα 2 : Έστω a_0 ,a_1 δύο διακριτοί πραγματικοί αριθμοί $r = [\log p]$ και ένα πολυώνυμο $f(X_1,\ldots, X_r) \in R[X_1,\ldots,X_r]$ τέτοιο ώστε $f(a_{u1},\ldots a_{ur}) \ge 0$ αν x είναι τετραγωνικό κατάλοιπο p και $f(a_{u1},\ldots a_{ur}) < 0$, αλλιώς όπου $x = u_1,\ldots u_r$ είναι η αναπαράσταση του x, $1 \le x \le 2^r - 1$.Τότε το f είναι βαθμού $\deg f \ge \log r + o(\log r)$ περιέχει τουλάχιστον $spr\ f \ge 0.25r + o(r)$.
Πόρισμα : Έστω το πολυώνυμο $f(X) \in R$ | X | που ικανοποιεί τις συνθήκες του Θεωρήματος 1 και του 2 , εξάγονται τα εξής συμπεράσματα :
(α) Υπάρχουν δύο RPNs που ‘’αντιλαμβάνονται’’ το πολυώνυμο f (X) και το $f(X_1,..,X_2)$
(β) Οι μέγιστες εντολές των κόμβων που περιλαμβάνει κάθε RPN πρέπει στην πρώτη περίπτωση να είναι ίσα με

$$\deg f(X) \geqslant \begin{cases} H/2 - 2s - 1 - p^{1/2}\log p, & for\ any\quad H, \\ \mathcal{C}(\varepsilon)\min\{H, H^2p^{-1/2}\} - 2s - 1, & if\quad p^{1/4+\varepsilon} \leqslant H \leqslant p^{1/2+\varepsilon}, \\ (p-1)/2 - 2s - 1, & if\quad N = 0, H = p-1, \end{cases}$$

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα αποτελέσματα των πειραμάτων για κάθε πρόβλημα έδειξαν ότι η διατύπωση και η παρουσίαση του προβλήματος είναι κρίσιμοι παράγοντες για την εκτέλεση των μεθόδων CI στην κρυπτογραφία. Ο σωστός ορισμός της αντικειμενικής συνάρτησης (fitness function συγκεκριμένα), όπως το να μη δημιουργούνται παραπλανητικές απεικονίσεις και διαγράμματα, είναι μείζονος σημασίας. Επίσης, η απόδοση των ΤΝΔ στα κρυπτογραφικά προβλήματα,

εξαρτάται από την μορφοποίηση του προβλήματος και την παρουσίαση των δεδομένων. Ένα δεύτερο συμπέρασμα είναι ότι οι μέθοδοι EC , γενικά οι μέθοδοι τεχνητής νοημοσύνης, χρησιμοποιούνται ως πρακτικές εκτίμησης της αποδοτικότητας και αποτελεσματικότητας των προτεινόμενων κρυπτογραφικών συστημάτων, αφού μπορούν να εντοπίσουν τα ελαττώματα των κρυπτογραφικών σχημάτων βρίσκοντας πρότυπα, πριν χρησιμοποιηθούν πιο περίπλοκες μέθοδοι για την ανάλυση τους.

ΚΕΦΑΛΑΙΟ 6ο : ΚΡΥΠΤΑΝΑΛΥΣΗ ΤΟΥ ΚΡΥΠΤΟΓΡΑΦΗΜΑΤΟΣ SPECK 32/64

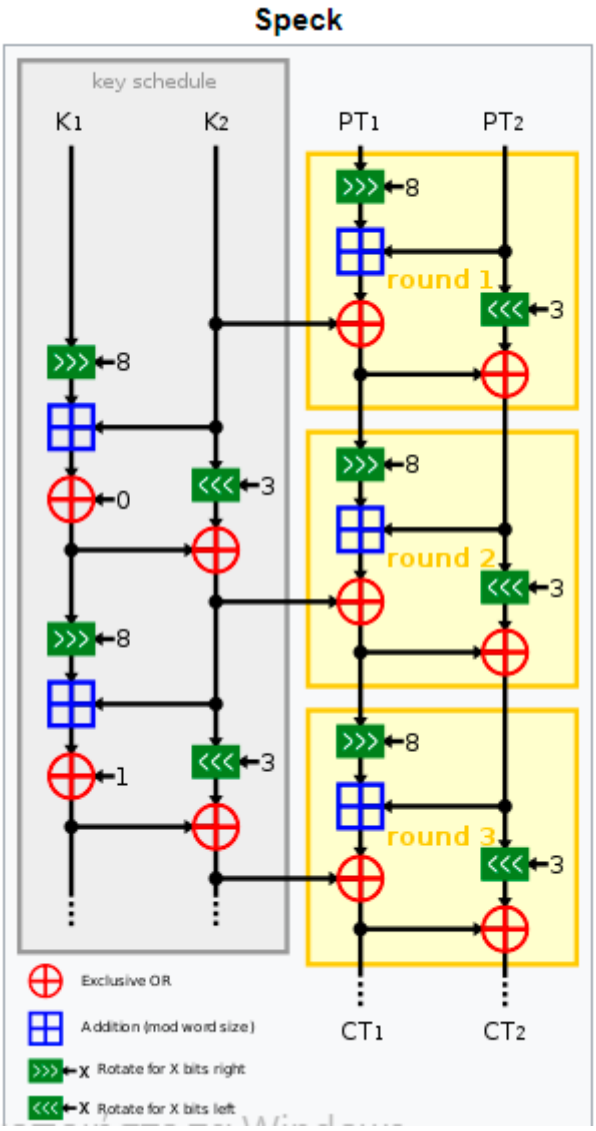
6.1. Τα Speck block ciphers

6.1.1 Περιγραφή του κρυπτογραφήματος Speck

Το speck block cipher είναι ένα επαναλαμβανόμενο κρυπτογράφημα, σχεδιασμένο από τους Beaulieu, Treatman-Clark, Shors, Weeks, Smith και Wingers για την National Security Agency, NSA, τον Ιούνιο του 2013. Ο στόχος τους ήταν να δημιουργηθεί ένα κρυπτογράφημα επαρκές για υλοποιήσεις λογισμικού σε συσκευές IoT (Internet of Things)[1].

Το Speck υποστηρίζει διάφορα μεγέθη block και μεγεθών κλειδιού. Ένα block είναι πάντα δύο λέξεις, αλλά οι λέξεις πρέπει να είναι 16,24,32,48 ή 64 bit. Το αντίστοιχο κλειδί να είναι 2,3 ή 4 λέξεων. Η κυκλική συνάρτηση αποτελείται από δύο περιστροφές, προσθέτοντας τη δεξιά λέξη στην αριστερή, xoring το κλειδί στην αριστερή, και μετά xor την αριστερή στη δεξιά λέξη. Ο αριθμός των επαναλήψεων εξαρτάται από τις επιλεγμένες παραμέτρους :

Block size (bits)	Key size (bits)	Rounds
2×16 = 32	4×16 = 64	22
2×24 = 48	3×24 = 72	22
	4×24 = 96	23
2×32 = 64	3×32 = 96	26
	4×32 = 128	27
2×48 = 96	2×48 = 96	28
	3×48 = 144	29
2×64 = 128	2×64 = 128	32
	3×64 = 192	33
	4×64 = 256	34



Είναι ένα κρυπτογράφημα ARX (Add- Rotate-Xor), που σημαίνει ότι είναι σύνθεση των βασικών συναρτήσεων όπως mod2^k , δυαδικής περιστροφής, δυαδικής προσθήκης σε λέξεις k-bit. Γενικά ένα Speck*n/m* , δηλώνει ένα Speck με n bit μέγεθος block και m bits μέγεθος κλειδιού.

Η συνάρτηση του Speck F: F_2^k x F_2^{2k} x → F_2^{2k} είναι πολύ απλή. Παίρνει ως είσοδο ένα k-bit δευτερεύον κλειδί K και ένα κρυπτογράφημα αποτελούμενο από δύο k-bit λέξεις (L_i, R_i) και παράγει την επόμενο κυκλικό στάδιο :

$$L_{i+1} := ((L_i \gg \alpha) \boxplus R_i) \oplus K, R_{i+1} := (R_i \ll \beta) \oplus L_{i+1},$$

Όπου α, β είναι συστατικά ειδικευμένα σε κάθε μέλος των κρυπτογραφημάτων speck (α=7,β=2 για Speck32/64 και α=8,β=3 για τις άλλες μεταβλητές). Η κυκλική συνάρτηση εφαρμόζεται προκαθορισμένες φορές (22 φορές στην περίπτωση του Speck 32/64) για να παράξει από την εισροή απλού κειμένου σε κρυπτογράφημα εκροής. Τα δευτερεύοντα κλειδιά για κάθε γύρο παράγονται από ένα κύριο κλειδί από ένα μη γραμμικό πρόγραμμα που χρησιμοποιεί ως κύριο block δόμησης την κυκλική συνάρτηση.

6.1.2 Κρυπτανάλυση του Speck

Αν και ελαφριάς κρυπτογράφησης, οι σχεδιαστές του Speck ισχυρίζονται ότι παρέχει την πλήρη δυνατή ασφάλεια για κάθε μπλοκ και μέγεθος κλειδιού, απέναντι σε επιθέσεις chosen-

plaintext (CPA) και chosen-ciphertext (CCA). Από το 2018, δεν είναι γνωστή κάποια επιτυχημένη κρυπτανάλυση σε Speck οποιοδήποτε μεταβλητών. Έχουν δημοσιευτεί πάνω από 70 έρευνες για την κρυπτανάλυση του. Όπως όλα τα επαναλαμβανόμενα κρυπτογραφήματα, οι μεταβλητές μειωμένων επαναλήψεων, έχουν δεχτεί επιτυχείς επιθέσεις. Οι καλύτερες δημοσιευμένες επιθέσεις του πρότυπου μοντέλου επίθεσης CPA-CCA είναι αυτές των διαφορικών επιθέσεων κρυπτανάλυσης (differential attacks) , πέτυχαν στο 70%-75% των επαναλήψεων των περισσότερων εκδοχών, ωστόσο είναι οριακά ταχύτερες από τις επιθέσεις ωμής βίας. Ο σχεδιαστής του Speck αναφέρει ότι κατά τη δημιουργία του, βρήκαν την επίθεση που τα κατάφερε στις περισσότερες επαναλήψεις , και όρισαν τον αριθμό των επαναλήψεων έτσι ώστε να υπάρχει ένα περιθώριο ασφαλείας παρόμοιο με τον AES 128, σε ποσοστό περίπου 30%.

Best known attacks on Speck (in standard attack model)

Variant	Rounds attacked	Time complexity	Data complexity	Space complexity	Attack type
Speck128/256	25/34 (74%)	$2^{253.35}$	$2^{125.35}$	2^{22}	differential[1]
Speck128/192	24/33 (73%)	$2^{189.35}$	$2^{125.35}$	2^{22}	differential[1]
Speck128/128	23/32 (72%)	$2^{125.35}$	$2^{125.35}$	2^{22}	differential[1]
Speck96/144	21/29 (72%)	$2^{143.94}$	$2^{95.94}$	2^{22}	differential[1]
Speck96/96	20/28 (71%)	$2^{95.94}$	$2^{95.94}$	2^{22}	differential[1]
Speck64/128	20/27 (74%)	$2^{125.56}$	$2^{61.56}$	2^{22}	differential[1]
Speck64/96	19/26 (73%)	$2^{93.56}$	$2^{61.56}$	2^{22}	differential[1]
Speck48/96	17/23 (74%)	$2^{95.8}$	$2^{47.8}$	2^{22}	differential[2]
Speck48/72	16/22 (73%)	$2^{71.8}$	$2^{47.8}$	2^{22}	differential[2]
Speck32/64	15/22 (68%)	$2^{63.39}$	$2^{31.39}$	2^{22}	differential[2]

Μία διαφορική επίθεση είναι μία κρυπτογραφική επίθεση που χρησιμοποιεί μη τυχαίες ιδιότητες της εκροής ενός κρυπτογραφικού πρωτότυπου, όταν του έχει δοθεί εισροή δεδομένων με γνωστή κατανομή διαφοράς. Η πιο γνωστή μορφή διαφορικής επίθεσης είναι πολλαπλές διαφορικές επιθέσεις, όπου οι πληροφορίες ενός αυθαίρετου συνόλου διαφορικών μεταβάσεων ερευνάται έτσι ώστε να μεγιστοποιηθεί το κέρδος της επίθεσης. Θα μελετήσουμε επιθέσεις που χρησιμοποιούν πληροφορίες που ανακτήθηκαν σε παρατηρούμενες διαφορές κρυπτοκειμένων (*purely differential*) και επιθέσεις όπου όλες οι πληροφορίες πάρθηκαν από τις εκροές των ζευγών των κρυπτογραφημάτων (*general differential*).

Ένας *distinguisher*[2] είναι ένας ταξινομητής C που δέχεται ως εισροή d δεδομένα από ανεξάρτητη δειγματοληψία από ένα ορισμένο σύνολο Ω ,σύμφωνα με μία από τις n διανομές πιθανοτήτων D_i , i=1,..,n και δίνει ως εκροή μία πρόβλεψη του i για την υποβαλλόμενη εισροή d. Σε αυτό το κεφάλαιο, το i επιλέγεται σε κάθε δοκιμή με πιθανότητα p_i από το σύνολο {1,2,..,n}. Η επιλεγόμενη μέθοδος για το i με τις κατανομές Di είναι γνωστή εκ των προτέρων και ονομάζεται πείραμα.

Το Speck έχει δεχτεί κριτική για το χαμηλό περιθώριο ασφαλείας του, λίγοι γύροι μεταξύ των καλύτερων επιθέσεων και του πλήρους κρυπτογραφήματος. Αυτά τα κρυπτογραφήματα είναι πιο πιθανό να ‘’σπάσουν’’ από μελλοντικές προόδους στην κρυπτανάλυση. Η σχεδιαστική ομάδα του Speck δηλώνει ότι το κόστος είναι πολύ μεγάλο για την μη απαραίτητη αύξηση των περιθωρίων ασφαλείας , ειδικά σε συσκευές μικρής κρυπτασφάλισης, ότι η κρυπτανάλυση κατά τη φάση του σχεδιασμού όρισε τις επαναλήψεις κατάλληλα και στόχευσαν το περιθώριο ασφάλειας του AES. Επίσης ισχυρίζονται ότι η NSA κρυπτανάλυση δεν βρήκε αδυναμίες στους

αλγόριθμους και ότι η ασφάλεια είναι ανάλογη του μεγέθους του κλειδιού και ότι χρησιμοποιήθηκε γραμμική και διαφορική κρυπτανάλυση.

Καθώς είναι ARX[3] κρυπτογράφημα, δεν χρησιμοποιεί S-boxes, οπότε είναι εκ των πραγμάτων απαραβίαστο από cache-time (εύρεσης χρόνου) επιθέσεις. Ωστόσο είναι ευάλωτο σε επιθέσεις power analysis[4] (ανάλυσης κατανάλωσης ενέργειας), εκτός αν έχουν παρθεί αντίμετρα υλικού. Τα Speck κρυπτογραφήματα έχουν μεταβλητές με μέγεθος μπλοκ και κλειδιού όπως ο AES (Speck 128/128, Speck 128/192, Speck 128/256), έχουν όμως και μεταβλητές με block μέγεθος 32 bit και μέγεθος κλειδιού 64 bits. Το πρόβλημα αυτών με τα μικρά μεγέθη block και κλειδιού είναι ότι είναι επισφαλή, παρά την επίσημη ασφάλεια του κρυπτογραφήματος. Μόνο η παραλλαγή των 128 bit size και 256 bit μέγεθος κλειδιού είναι εγκεκριμένο από την U.S. National Security Systems.

6.2 Πολλαπλές Διαφορικές Επιθέσεις σε Speck32/64

6.2.1 Αμιγώς διαφορικοί ''Διακριτές''

Οι πολλαπλές διαφορικές επιθέσεις δημιουργούν κρυπτογραφικούς διαχωριστές (distinguishers) χρησιμοποιώντας ένα σύνολο S διαφορικών μεταβάσεων για κάποια κρυπτογραφική συνάρτηση F για να χαρακτηρίσει την συμπεριφορά της. Η βασική ιδέα είναι ότι κάθε μετάβαση $\Delta_i \rightarrow \delta_j$ στο S, έχει συσχετιστεί με μία πιθανότητα p_{ij} να γίνει αντιληπτή, δοθέντων των ρυθμίσεων του πειράματος του κρυπτογραφήματος που μελετάται και μια άλλη πιθανότητα $\sim p_{ij}$ σε κάποια περίπτωση να διαχωριστεί αντίθετα.

Υπολογίζοντας πιθανότητες διαφορικών μεταβάσεων :Χρησιμοποιούμε έναν αλγόριθμο για να υπολογίσουμε τα μη γραμμικά συστατικά του Speck32/64, που είναι μία απλή αρθρωτή προσθήκη modulo 2^{16} . Έτσι έχουμε έναν αποτελεσματικό τρόπο για πρόσβαση σε αυθαίρετες εισόδους του μιας επανάληψης διαφορικής μετάβασης πίνακα $A \in R^{2^{32} \times 2^{32}}$ του Speck. Δοθείσας μία εισροής διαφορικής κατανομής $u_i \in R^{2^{32}}$ για τον γύρο i του Speck , υπολογίζουμε την κατανομή της εισροής του γύρου i+1 θέτοντας $u_{i+1} \equiv A_{ui.}$

Οι κρυπτογραφικοί στόχοι είναι να διαχωριστεί η εκροή του Speck με τη Δ διαφορά εισροής μειωμένων επαναλήψεων από τα τυχαία δεδομένα. Οι distinguishers θα χρησιμοποιήσουν την πλήρη προβλεπόμενη εκροή διανομή διαφοράς για τον θεωρούμενο αριθμό επαναλήψεων. Ορίζουμε ως D_i το αποτέλεσμα του ''διακριτή'' για την i επανάληψη. Π.χ. D5 είναι το αποτέλεσμα πέντε επαναλήψεων και το αντίστοιχο πρόβλημα θα αναφέρεται ως D5 task.

Κατηγοριοποίηση : Για να γίνει ο διαχωρισμός των πραγματικών ζευγών κρυπτοκειμένου και παραδειγμάτων που παράγονται τυχαία, υποθέτουμε ότι τυχαία ζεύγη κρυπτοκειμένου διανέμονται σύμφωνα με την ομοιόμορφη κατανομή σε μη μηδενικές δέσμες κρυπτοκειμένων. Κατηγοριοποιούμε μία παρατηρούμενη διαφορά δ εκροής ως πραγματική αν η πιθανότητα που προβλέφθηκε και αφορά στην παρατήρηση της στην πραγματική κατανομή είναι $> 1/(2^{32} - 1)$ και ως τυχαία για την αντίθετη περίπτωση. Αυτό εκμεταλλεύεται πλήρως την ανομοιομορφία της εκροής της συνάρτησης διαφοράς αν η πρόβλεψη μας για αυτή την κατανομή δεν περιλαμβάνει λάθη. Οι αναφερόμενες αληθείς θετικές τιμές για τους distinguishers ορίζονται από την προβλεπόμενη εκροή διανομής που υπολογίστηκε υπό την προϋπόθεση ότι η πραγματική εκροή, είναι αυτή που προβλέφθηκε.

Πηγές λάθους : Οι υπολογισμοί αυτού του είδους δουλεύουν μόνο αν το κρυπτογράφημα δεν διαφέρει πολύ από το Markov. Το μοντέλο ελέγχεται με τρείς τρόπους:

1. Τεστάραμε εμπειρικά ότι η υψηλότερη πιθανότητα μετάβασης που βρέθηκε για το μοντέλο μας για οκτώ γύρους (0x0040/0000 →0x0280/0080) εμπειρικά παρατηρείται με την αναμενόμενη πιθανότητα $2^{-26.015.}$
2. Επίσης, οι προβλεπόμενες αληθείς θετικές τιμές των διαφορικών distinguishers ταιριάζουν με παρατηρηθείσες τιμές σε ένα μέγεθος 10^6 συνόλου δοκιμών από την πραγματική κατανομή. Αυτή είναι και η περίπτωση μέσα στα πειράματα περιθωρίων λάθους. Το αντίστοιχο πείραμα για αληθείς αρνητικές τιμές δεν έγινε, γιατί η τυχαία κατανομή είναι γνωστή εκ των προτέρων, οπότε δοθέντος του distinguisher , δεν υπάρχει λάθος στην πρόβλεψη της ακρίβειας του σε τυχαία δείγματα.
3. Χρησιμοποιήθηκαν στην έρευνα 100 δις δείγματα σε κάθε περίπτωση, για την προσέγγιση της διαφοράς κατανομής του Speckk 32/64. Τα αποτελέσματα ήταν καθαρά χαμηλότερα από το θεωρητικό μοντέλο.

Τα πειράματα δείχνουν ότι το μοντέλο συλλαμβάνει την διαφορετική κατανομή του Speck 32/64 αρκετά καλά.

6.2.2 Διαφορικοί ‘’distinguishers’’ με χρήση πλήρους κατανομής των ζευγών κρυπτοκειμένων

Οι ‘’διακριτές΄΄ που μελετώνται παρατηρούν ένα ζεύγος κρυπτοκειμένων που παράγεται από μία γνωστή εισροή διαφορά (τα απλά κείμενα δεν είναι γνωστά) και προσπαθούν να μαντέψουν βασιζόμενοι στη διαφορά των κρυπτοκειμένων αν το ζεύγος που μελετάμε έχει παραχθεί από κρυπτογράφηση Speck μειωμένων επαναλήψεων ή τυχαία. Η όλη τεχνική μπορεί να βελτιωθεί αν μελετήσουμε όλα τα δεδομένα, και όχι μόνο τα δεδομένα της διαφοράς. Αυτό βέβαια, δεν είναι εφικτό. Σκοπός είναι να καθοριστεί για διαφορικούς ‘’distinguishers’’ σε Speck 5 επαναλήψεων κατά πόσο θα είναι πλεονέκτημα των αντιπάλων η εξερεύνηση αυτών των περαιτέρω πληροφοριών.

Ο τέλειος distinguisher για το D5 (Speck32/64): Δοθέντος ενός ζεύγους κρυπτοκειμένου C: = (C_0, C_1) και εισροή μία διαφορά Δ , η πιθανότητα P(C|real) να παρατηρηθεί (C_0 ,C_1) στην πραγματική κατανομή για ένα κρυπτογραφικό αλγόριθμο δέσμης E μεγέθους block b και μέγεθος κλειδιού k δοθέντος τυχαίο κλειδί και τα δεδομένα του απλού κειμένου δίνεται από $2^{-(b+k)}$N , όπου N είναι ο αριθμός του κλειδιού και ζευγάρια απλού κειμένου (K,P) τέτοια ώστε E_K (P) = C_0 και $E_κ$ (P ⊕ Δ) =C_1. Το N είναι ο αριθμός N_{keys} (C) κλειδιών που αποκρυπτογραφούν το C με διαφορά Δ. Αντίθετα, P(C|random)=1/(2^{2b} -2^b) ,εφαρμόζουμε το θεώρημα Bayes’ ,για την τέλεια ταξινόμηση, πρέπει να καθορίσουμε αν

$$N_{\text{keys}}(C) > 2^{b+k}/(2^{2b} - 2^b) \approx 2^{b+k-2b}$$

ή όχι. Για το Speck32/64 ελέγχουμε αν0020 $N_{keys} > 2^{32}$. Για το σκοπό D5 στην πράξη, απαριθμούμε τις πιθανές διαφορικές καταστάσεις του γύρου-3 και κάνουμε επίθεση 2 επαναλήψεων για κάθε μία από αυτές τις ενδιάμεσες διαφορές, απαριθμίζοντας τα δευτερεύοντα κλειδιά sk_5 και sk_4 που χρησιμοποιήθηκαν στον γύρο 4 και 5. Αφού πάρουμε την εκροή του γύρου 3, σημειώνουμε ότι η διαφορά εκροής του γύρου 1 είναι γνωστή και χρησιμοποιούμε την επίθεση δύο γύρων για να ανακτήσουμε τα δύο πρώτα δευτερεύοντα κλειδιά. Σταματάμε μετά από 2^{32} +1 λύσεις ή αν έχουμε εξαντλήσει το χώρο του κλειδιού, ό,τι προκύψει πρώτο. Δοκιμάστηκε σε 1000 παραδείγματα, εκ των οποίων τα 9456 ήταν σωστά ταξινομημένα, με συνολικό ποσοστό ακρίβειας 95 %. Αντικαθιστώντας την έρευνα για το κλειδί με μία πολύ πιο γρήγορη εκτίμηση του αριθμού των λύσεων βασιζόμενη στον πίνακα κατανομής διαφοράς 3 γύρων δεν οδήγησε σε σημαντική στατιστική μείωση της εκτέλεσης.

6.3 Νευρωνικοί distinguishers

6.3.1 Αρχιτεκτονική Δικτύου

Αναπαράσταση Εισροών: Ένα ζευγάρι (C_0, C_1)ζευγών κρυπτοκειμένων για τον Speck32/64 μπορεί να γραφτεί ως μία αλληλουχία από λέξεις 16 bit (w_0,w_1,w_2,w_3) αντικατοπτρίζοντας την προσανατολισμένη στη λέξη αρχιτεκτονική του κρυπτογραφήματος. Το w_i μεταφράζεται ως διανύσματα σειράς ενός 4 x 16 πίνακα και το επίπεδο εισροής αποτελείται από 64 μονάδες ταξινομημένες σε πίνακα 4 x 16.

Συνολική αρχιτεκτονική δικτύου: Το ιδανικό είναι ένας residual[5] (υπολειπόμενος) πύργος από δύο convolutional[6] συνελικτικά νευρωνικά δίκτυα ενώ έχει προηγηθεί ένα μοναδικό bit-sliced και ακολουθούμενα από μία πυκνά συνδεδεμένη κεφαλή προβλέψεων. Το εσωτερικό επίπεδο συνδέεται με ένα bit-sliced[7] ,πχ το πλάτος 1 συνδέεται με 32 κανάλια εκροής. Η ομαλοποίηση της δέσμης γίνεται στην εκροή αυτών των περιελίξεων. Στο τέλος εφαρμόζονται μη γραμμικοί ανορθωτές στις εκροές αυτών και το αποτέλεσμα είναι ένας πίνακας 32 x 16 που συνδέεται στο κύριο πύργο. Κάθε συνελικτικό μπλοκ αποτελείται από δύο επίπεδα 32 φίλτρων. Κάθε επίπεδο εφαρμόζει πρώτα τους περιελιγμούς, μετά την ομαλοποίηση της δέσμης και τέλος ένα στρώμα επανόρθωσης. Στο τέλος του συνελικτικού μπλοκ, ένας σύνδεσμος προσθέτει την εκροή του τελικού επιπέδου επανόρθωσης του μπλοκ στην εισροή του και περνάει το αποτέλεσμα στο επόμενο μπλοκ.

Κεφαλή πρόβλεψης : Αποτελείται από δύο κρυμμένα επίπεδα και μία μονάδα εκροής. Το πρώτο και το δεύτερο επίπεδο είναι πυκνά συνδεδεμένα επίπεδα με 64 μονάδες. Το πρώτο ακολουθείται από ένα επίπεδο ομαλοποίησης δέσμης και ένα επανόρθωσης , το δεύτερο δεν χρησιμοποιεί ομαλοποίηση δέσμης αλλά είναι απλά ένα πυκνά συνδεδεμένο επίπεδο από 64 μονάδες. Το τελευταίο επίπεδο αποτελείται από μία μόνο μονάδα εκροής που χρησιμοποιεί σιγμοειδή ενεργοποίηση.

Αιτιολόγηση δομής: Η χρήση του εσωτερικού επιπέδου πλάτους-1 έχει στόχο να κάνει τη μάθηση απλών συναρτήσεων bit-sliced ευκολότερη. Ο αριθμός των φίλτρων στο εσωτερικό επεκτείνουν τα δεδομένα στη μορφή που απαιτείται από τον υπολειπόμενο (residual) πύργο. Η επιλογή των εσωτερικών καναλιών προκύπτει από την επιθυμία να γίνει ο προσανατολισμός λέξεων του κρυπτογραφήματος στο δίκτυο. Η χρήση πυκνά συνδεδεμένων κεφαλών προβλέψεων αντικατοπτρίζει το γεγονός ότι για μη ασήμαντο αριθμό γύρων, δεν αναμένεται τα δεδομένα εισροής να δείξουν δυνατές χωρικές συμμετρίες, έτσι οποιαδήποτε προσπάθεια εξόρυξης τοπικών χαρακτηριστικών από τα δεδομένα χρησιμοποιώντας ένα χωρικό συμμετρικό επίπεδο συγκέντρωσης είναι πιθανώς ανωφελής. Το μέγεθος των στρωμάτων καθορίστηκε από πείραμα. Το βάθος του υπολειπόμενου πύργου επιλέχθηκε ώστε να επιτραπεί η ενσωμάτωση των δεδομένων εισροής στην συμβολοσειρά εισόδου μεταξύ των συνελικτικών επιπέδων. Ωστόσο, και σχεδιασμός ενός και μόνο υπολειπόμενου block φέρνει καλά αποτελέσματα.

6.3.2 Ταξινομητές (Classifiers)

Παραγωγή δεδομένων: Τα δεδομένα εκπαίδευσης και αξιολόγησης παράχθηκαν από την Linux γεννήτρια τυχαίων αριθμών για να αποκτηθούν ομοιόμορφα κατανεμημένα κλειδιά K_i και ζεύγη απλών κειμένων P_i με την διαφορά εισροής Δ=0x0040/0000 όπως και ένα διάνυσμα δυαδικής αξίας τυχαίων ετικετών Y_i. Για την παραγωγή δεδομένων εκπαίδευσης ή αξιολόγησης για Speck k επανάληψης, το P_i κρυπτογραφήθηκε για k επαναλήψεις αν το Y_i έχει ρυθμιστεί,

αλλιώς το δεύτερο απλό κείμενο του ζεύγους αντικαθίσταται με ένα νέο τυχαίο. Με αυτό τον τρόπο, σύνολα δεδομένων αποτελούμενα από 10^7 δείγματα παράχθηκαν για εκπαίδευση. Η προ-επεξεργασία έγινε για να μετατραπούν τα δεδομένα στην απαιτούμενη μορφή για το δίκτυο.
Εκπαίδευση : Ένα σύνολο δεδομένων μεγέθους 10^7 εκπαιδεύτηκε για 200 ΄΄εποχές΄΄. Η επεξεργασία έγινε σε δέσμες μεγέθους 5000. Τα τελευταία 10^6 δείγματα παρακρατήθηκαν για αξιολόγηση. Η βελτιστοποίηση έγινε στην μέση απώλεια σφάλματος τετραγώνου με τον αλγόριθμο Adam. Χρησιμοποιήθηκε ένα κυκλικό ποσοστό εκμάθησης

$$l_i := \alpha + \frac{(n-i) \bmod (n+1)}{n} \cdot (\beta - \alpha),$$

Με $\alpha=10^{-4}$, $\beta=2'10^{-3}$ και n= 9. Τα δίκτυα που ελήφθησαν στο τέλος κάθε ΄΄εποχής΄΄ αποθηκεύτηκαν και το καλύτερο δίκτυο αξιολογήθηκε απέναντι σε ένα σύνολο δοκιμών μεγέθους 10^6 που δεν χρησιμοποιήθηκε σε εκπαίδευση ή αξιολόγηση.

Έγινε έλεγχος για το αν η έρευνα κλειδιού μπορεί να βελτιώσει τους distinguishers. Η μέθοδος φαίνεται στον παρακάτω αλγόριθμο.

Algorithm 1 KeyAveraging: Deriving a differential distinguisher against a block cipher E^{r+1} reduced to $r+1$ rounds for input difference Δ from a corresponding distinguisher $\mathcal{D}$ against E^r. A sample is predicted to come from the real distribution if and only if the output value of the algorithm is ≥ 0.5.

Require: Observed output ciphertext pair $C_0, C_1 \in \{0,1\}^b$
1: $D_i \leftarrow [\text{DecryptOneRound}(C_i, k) \text{ for } k \in \text{Subkeys}]$
2: $v_k \leftarrow \mathcal{D}(D_0[k], D_1[k])$ for all $k \in$ Subkeys
3: $v_k \leftarrow v_k/(1-v_k)$ for all $k \in$ Subkeys
4: $v \leftarrow \text{Average}([v_k, k \in \text{Subkeys}])$
5: $v \leftarrow v/(1+v)$
6: **return** v

Εκπαίδευση distinguisher για 8 επαναλήψεις: Το παραπάνω σχήμα αποτυγχάνει για 8 επαναλήψεις. Για αυτό το λόγο χρησιμοποιήθηκαν στάδια προ-εκπαίδευση. Πρώτα επανεκπαιδεύουμε τους καλύτερους distinguisher εφτά γύρων να αναγνωρίζουν Speck32/64 5 γύρων με εισροή διαφορά 0x8000/840a. Αυτό έγινε σε 10^7 για 10 epochs με μέγεθος δέσμης 5000 και ποσοστό εκμάθησης 10^{-4} . Μετά, εκπαιδεύουμε τους distinguisher που έχουμε αποκτήσει να αναγνωρίζουν Speck 8 γύρων με εισροή διαφορά 0x0040/0000 επεξεργάζοντας 10^9 νέα παραδείγματα με μέγεθος δέσμης 10000, με συνεχές τον ρυθμό εκμάθησης. Τελικά, αυτός ο ρυθμός έπεσε δύο φορές στο 10^{-5} και τελικά στο 10^{-6} αφού επεξεργάστηκαν άλλα 10^9 νέα παραδείγματα, με ίδιο μέγεθος δέσμης.

Αποτελέσματα: Οι νευρικοί distinguisher πετυχαίνουν μεγαλύτερη ακρίβεια από ότι οι βασικοί. Η ακρίβεια των βασιζόμενων στην αναζήτηση κλειδιού distinguishers δεν ταίριαζαν.

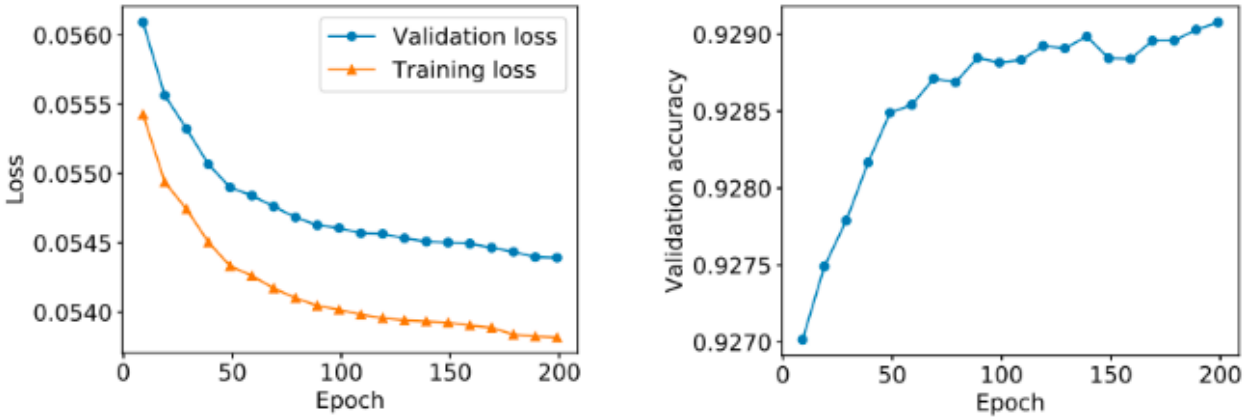


Fig. 1. Training a neural network to distinguish 5-round Speck32/64 output for the input difference $\Delta = 0x0040/0$ from random data. *(left)* Training and validation loss by epoch. *(right)* Validation accuracy. *(both)* Only data for epochs with lowest learning rate is shown. Intermediate epochs contained excursions to low performance. Full learning history for this run is available from supplementary data.

Χρησιμοποιώντας το γεγονός ότι η πρώτη προσθήκη δευτερεύοντος κλειδιού συμβαίνει μετά την πρώτη εφαρμογή μη γραμμικότητας στο Speck, μπορούμε να επεκτείνουμε κατά ένα γύρο τους distinguishers, χωρίς επιπλέον κόστος. Μία απλή επίθεση σε 9-round Speck γίνεται ως εξής:

1. Αναζητούμε κρυπτογράφηση για n ζεύγη P_1 ,..,P_n τέτοια ώστε η εκροή διαφορά του πρώτου γύρου να είναι Δ=0x0040/0000. Βρίσκουμε τα κρυπτογραφημένα ζεύγη C_1, ..,C_n.
2. Για κάθε τιμή του τελικού δευτερεύοντος κλειδιού k, αποκρυπτογραφούμε το C_i με το k, για να πάρουμε το C_i^k .δ_i^k είναι η διαφορά του ζεύγους C_i^k .
3. Χρησιμοποιούμε ένα διαφορικό distinguisher 7- γύρων για να πάρουμε τιμές Z_i^k για κάθε αποκρυπτογραφημένο ζεύγος.
4. Για κάθε k, συνδυάζουμε Z_i^k σε ένα σύνολο υ_k.
5. Κατατάσσω τα κλειδιά σε φθίνουσα σειρά σύμφωνα με το υ_k τους.

Στον παρακάτω πίνακα παρουσιάζεται η ακρίβεια διάφορων distinguishers ενάντια στο Speck32/64 , χρησιμοποιώντας δύο μπλοκ κρυπτοκειμένων με επιλεγμένη διαφορά απλού κειμένου 0x0040/0000 για N_r γύρους.

Nr	Distinguisher	Accuracy	True Positive Rate	True Negative Rate
5	D5	0.911	0.877	0.947
5	N5	$0.929 \pm 5.13 \cdot 10^{-4}$	$0.904 \pm 8.33 \cdot 10^{-4}$	$0.954 \pm 5.91 \cdot 10^{-4}$
6	D6	0.758	0.680	0.837
6	N6	$0.788 \pm 8.17 \cdot 10^{-4}$	$0.724 \pm 1.26 \cdot 10^{-3}$	$0.853 \pm 1.00 \cdot 10^{-3}$
7	D7	0.591	0.543	0.640
7	N7	$0.616 \pm 9.7 \cdot 10^{-4}$	$0.533 \pm 1.41 \cdot 10^{-3}$	$0.699 \pm 1.30 \cdot 10^{-3}$
8	D8	0.512	0.496	0.527
8	N8	$0.514 \pm 1.00 \cdot 10^{-3}$	$0.519 \pm 1.41 \cdot 10^{-3}$	$0.508 \pm 1.42 \cdot 10^{-3}$

D5-D8 είναι κλασσικοί διαφορικοί distinguishers που χρησιμοποιούν όλη τον πίνακα κατανομής διαφορών του Speck32/64 (calculated under the Markov assumption). N5-N8 είναι νευρικοί distinguishers. Οι ακρίβειες των D5-D8 distinguishers είναι θεωρητικές προβλέψεις βασιζόμενες στην υπόθεση ότι σωστά μάντεψαν την κατανομή διαφοράς, με εμπειρικά επιβεβαιωμένο 2σ error περιθώριο σε μέγεθος 10^6 σύνολα δοκιμών. Οι αριθμοί των νευρικών distinguishers

πάρθηκαν με δοκιμές μεγέθους 106 συνόλων δοκιμών με περίπου περιεχόμενο 500000 θετικά και αρνητικά παραδείγματα το καθένα. N5 και N6 είναι δίκτυα με 10 υπολειπόμενα μπλοκ, ενώ N7 and N8 είναι μικρότερα δίκτυα με μόνο ένα μπλοκ.
Στην περίπτωση των νευρικών distinguisher , χρησιμοποιούμε:

$$v_k := \sum_{i=1}^{n} \log_2(Z_i^k/(1-Z_i^k))$$

,για τον συνδυασμό των σκορ του κάθε αποκρυπτογραφημένο ζεύγος σε ένα για το κλειδί. Στην περίπτωση του πίνακα κατανομής διαφοράς :

$$v_k := \sum_{i=1}^{n} \log_2(P(\delta_i^k)),$$

Όπου $P(\delta_i^k)$ είναι η πιθανότητα να παρατηρήσουμε εκροή διαφοράς δ_i^k στην εκροή του Speck32/64 7 γύρων με εισροή τη διαφορά Δ.
Επιλέχθηκε n=64 για το πείραμα. Με αυτή τη ρύθμιση, οι νευρικοί distinguishers κατάφεραν καλύτερη ταξινόμηση κλειδιών.

Distinguisher	Mean of key rank	Median key rank	Success rate
D7	263.9 ± 77.7	9.0	0.13
N7	52.1 ± 34.7	1.0	0.358

Αυτές είναι οι στατιστικές στην ανάκτηση κλειδιών σε Speck32/64 9 γυρών. Η ίδια επίθεση χρησιμοποιώντας 128 επιλεγμένα απλά κείμενα πραγματοποιήθηκε με distinguisher βασισμένο σε πίνακα κατανομής διαφοράς και με νευρικό ενάντια σε Speck32/64 μειωμένο σε 7 γύρους. Όλες οι τιμές βασίστηκαν σε 1000 δοκιμές των επιθέσεων. Οι γραμμές σφάλματος γύρω από τον μέσο είναι για 2σ διάστημα εμπιστοσύνης, όπου σ υπολογίζεται βασισμένο στην απόκλιση της ταξινόμησης κλειδιού. Η ταξινόμηση του κλειδιού ορίζεται ως ο αριθμός των δευτερευόντων κλειδιών που ταξινομήθηκαν ψηλότερα. Όταν πολλά κλειδιά έχουν την ίδια κατάταξη, το σωστό κλειδί είναι κάπου τυχαία ανάμεσα τους.

Πρόταση 1: Έστω ότι E είναι οποιοδήποτε Speck με ελεύθερο πρόγραμμα κλειδιού και A είναι μία επίθεση που προσπαθεί να ανακτήσει το κλειδί χρησιμοποιώντας καθαρά διαφορικούς μεθόδους , πχ λαμβάνει ως εισροή $P_0 \oplus P_1 \oplus P_2$,.., $P_o \oplus P_n$ όπως και κρυπτοκείμενα C_0, C_1,.., C_n. Τότε η πλήρης ανάκτηση κλειδιού δεν θα είναι ποτέ επιτυχής με ποσοστό επιτυχίας μεγαλύτερο του 50%.

Απόδειξη: Υποθέτουμε ότι $E^{-1}_{\kappa}(C_0) \oplus E^{-1}_{\kappa}(C_1) = \delta$, όπου E_κ δηλώνει κρυπτογράφηση μονής επανάληψης με το δευτερεύων κλειδί k. Ανατρέποντας το πιο σημαντικό bit του k και το νέο κλειδί k'. Έπειτα πρέπει να αποδείξουμε ότι $E^{-1}_{k}(C_0) \oplus E^{-1}_{k}(C_1) = \delta$. Ως εκ τούτου, οι καθαρά διαφορικοί distinguishers για Speck πάντα παράγουν ζεύγη ισάξια κατανεμημένων δευτερευόντων κλειδιών μέχρι να αποκλειστούν από το πρόγραμμα υποψήφια κλειδιά.

Για Speck32/64 παράχθηκαν 1εκ. δοκιμαστικά σύνολα και υπολογίστηκε η σχετική είσοδος του πίνακα κατανομής διαφοράς για Speck32/64 και η εκροή ενός 5-γύρων ενός block νευρωνικής πρόβλεψης. Τα μισά από τα δείγματα του τεστ παράχθηκαν με κανονική κατανομή και το άλλο μισό τυχαία. Η μελέτη έγινε για να μελετηθούν οι διαφορές μεταξύ νευρωνικής πρόβλεψης και του διαφορετικού πίνακα διανομής. Η διαφορά μεταξύ των δύο προβλέψεων παρατηρήθηκε σε 48826 δείγματα, εκ των οποίων η πληθώρα ήταν από την τυχαία κατανομή (περίπου 57%). Το νευρωνικό μας δίκτυο επέλεξε την ταξινόμηση που αντιστοιχεί στην πραγματικότητα κατά 67% στις περιπτώσεις διαφωνίας. Ωστόσο η εκμετάλλευση των πληροφοριών που αποκτώνται αξιόπιστα από τον πίνακα διανομής διαφοράς δεν είναι τέλεια.

Για παράδειγμα, 1549 από τα δείγματα, ανταποκρίθηκαν σε αδύνατες διαφορικές μεταβάσεις. Δύο από αυτά ταξινομήθηκαν λάθος από το νευρικό δίκτυο προερχόμενα από την κανονική κατανομή, αν και στις δύο περιπτώσεις το επίπεδο εμπιστοσύνης που είχε εκροή το νευρικό δίκτυο ήταν χαμηλό (56% και 53%). Όμως, το νευρικό δίκτυο αναγνώρισε ζευγάρια εκροής που δε θα είχαν εμφανιστεί στην κανονική κατανομή.

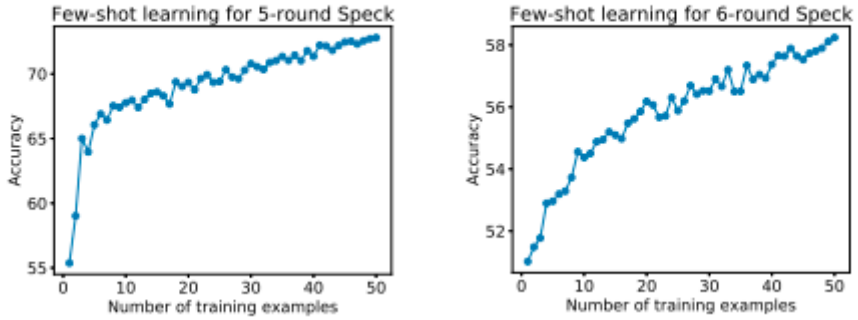
Few-shot Learning Κρυπτογραφικών Διανομών: Few-shot learning είναι η ικανότητα ανθρώπων ή μηχανών να μαθαίνουν να αναγνωρίζουν αντικείμενα συγκεκριμένης κατηγορίας ή να λύνουν συγκεκριμένα προβλήματα ενώ έχουν δει μόνο ένα ή ελάχιστα παραδείγματα. Έγιναν δοκιμές για το αν τα νευρωνικά δίκτυα μπορούν επιτυχώς να το εφαρμόσουν σε μία κρυπτογραφική διανομή έχοντας γνώση από μία άλλη σχετική διανομή εκτελώντας το εξής πείραμα : ένα νέο νευρωνικό δίκτυο με ένα μπλοκ εκπαιδεύτηκε πρώτα να αναγνωρίζει Speck 3 γύρων με μία προκαθορισμένη αλλά τυχαία επιλεγμένη διαφορά εισροή. Η εκπαίδευση αποτελούνταν από μία epoch 2000 καθοδικών βημάτων με μέγεθος δείγματος 5000, για το οποίο απαιτήθηκε 1 λεπτό χρόνου. Έπειτα φτάσαμε την εκροή του δεύτερου ως τελευταίου στρώματος , συμπεριφερόμενοι σαν αν είναι μια αναπαράσταση των δεδομένων εισροής. Παράχθηκαν μικρά δείγματα από την εκροή κατανομής για έξι γύρους του Speck με επιλεγμένη εισροή την διαφορά των κύριων distinguishers.Κάθε σύνολο παραδείγματος συμπληρώθηκαν από τον ίδιο αριθμό δειγμάτων που προέρχονται από την τυχαία διανομή. Το αποτέλεσμα ήταν το σύνολο παραδειγμάτων S και στάλθηκε στο νευρωνικό δίκτυο για να ανακτήσει το αντίστοιχο σύνολο S’ $\subset R^{64}$ των εσωτερικών διανυσμάτων. Η παλινδρόμηση κορυφογραμμών χρησιμοποιήθηκε για να δημιουργήσει από αυτό το μικρό σύνολο μία γραμμική πρόβλεψη $L : R^{64} \rightarrow R$ για 6 γύρων διανομή ελαχιστοποιώντας το τετράγωνο λάθους μεταξύ προβλέψεων και ετικετών S’. Ταξινομούμε ένα παράδειγμα $x \in S'$ ως αληθή αν $L(x) > 0.5$ και ως τυχαία αντίθετα. Αυτή η πρόβλεψη δοκιμάστηκε σε ένα μέγεθος 50000 συνόλου δοκιμών για να καθοριστεί η ακρίβεια του.

Algorithm 2 TrainByTransfer: Training a distinguisher for a block cipher with block size b reduced to r rounds E^r with input difference δ by transfer learning given an auxiliary neural distinguisher N for input difference Δ and E^s.

Require: N, r, δ, n

1: $X_0 \leftarrow n$ samples drawn from the real output distribution of E^r with input difference δ.
2: $Y_0 \leftarrow (1, 1, ..., 1) \in \mathbb{R}^n$
3: $X_1 \leftarrow n$ samples drawn uniformly at random from $\{0,1\}^{2b}$.
4: $Y_1 \leftarrow 0 \in \mathbb{R}^n$.
5: $N' \leftarrow N[-2]$, where $N[-2]$ denotes the output of the second-to-last layer of N.
6: $Z, Y \leftarrow N'(X_0||X_1), Y_0||Y_1$
7: $L \leftarrow \text{RidgeRegression}(Z, Y)$
8: **return** $L \circ N'$

Παρακάτω βλέπουμε few-shot εκμάθηση για D5 και D6 tasks, έχοντας χρησιμοποιήσει προ-εκπαιδευμένο ταξινομητή για να προ-επεξεργαστεί τα δεδομένα εισροής. Ο αλγόριθμος 2 χρησιμοποιήθηκε με ένα σταθερό εκπαιδευμένο δίκτυο να ξεχωρίζει Speck32/64 μειωμένο σε 3 γύρους με τυχαίες καθορισμένες διαφορές ως εισροή. Ο αριθμός των παραδειγμάτων ποίκιλλε από 1 ως 50. Οι απεικονίσεις ακρίβειας είναι ένας μέσος όρος πάνω από 100 ‘’τρεξίματα’’ για κάθε εκπαιδευτικό μέγεθος. Η ακρίβεια μετρήθηκε ενάντια σε ένα καθορισμένο σύνολο μεγέθους 50000.



Χάρη στη few-shot εκμάθηση μπορούμε, δοθέντος ενός προ-εκπαιδευμένου δικτύου για Speck 3 επαναλήψεων και μίας τυχαίας εισροής διαφοράς δ, να εκπαιδεύσουμε ταχέως έναν distinguisher για μία άλλη τυχαία διαφορά δ΄ ως εισροή και να αξιολογηθεί η ακρίβεια τους με ένα μικρό σύνολο δοκιμών. Ξεκινώντας από ένα τυχαίο δ΄, χρησιμοποιούμε τον αλγόριθμο 3 για να βελτιστοποιήσουμε δ΄ για την ακρίβεια του συνόλου δοκιμών των distinguishers που προέκυψαν. Χρησιμοποιώντας α= 0.01, t= 2000 και σύνολα δεδομένων μεγέθους 1000 για κάθε νέα διαφορά ως εισροή που είναι για δοκιμή , χρειάζονται λιγότερο από 2 λεπτά χρόνου υπολογισμού για την εκπαίδευση των εσωτερικών 3 γύρων distinguishers και περίπου 15 δευτερόλεπτα για μία πλήρη εκτέλεση του αλγόριθμου 3.

Algorithm 3 GreedyOptimizerWithExplorationBias: Given a function $F : \{0,1\}^b \to R$, try to find $x \in \{0,1\}^b$ which maximises F.

Require: F, number t of iterations, exploration factor α, input bit size b

$x \leftarrow \text{Rand}(0, 2^b - 1)$
$v_{\text{best}} \leftarrow F(x)$
$x_{\text{best}} \leftarrow x$
$v \leftarrow v_{\text{best}}$
$H \leftarrow$ hashtable with default value 0
for $i \in \{1, \ldots, t\}$ **do**
  $H[x] \leftarrow H[x] + 1$
  $r \leftarrow \text{Rand}(0, b - 1)$
  $x_{\text{new}} \leftarrow x \oplus (1 \ll r)$
  $v_{\text{new}} = F(x_{\text{new}})$
  if $v_{\text{new}} - \alpha \log_2(H[x_{\text{new}}]) > v - \alpha \log_2(H[x])$ **then**
    $v, x \leftarrow v_{\text{new}}, x_{\text{new}}$
  end if
  if $v_{\text{new}} > v_{\text{best}}$ **then**
    $v_{\text{best}}, x_{\text{best}} \leftarrow v, x$
  end if
end for
return x_{best}

6.4 Επίθεση Ανάκτησης Κλειδιού

Η έρευνα που παρουσιάζεται σε αυτό το κεφάλαιο, κατασκεύασε μία επίθεση ανάκτησης μερικού κλειδιού βασιζόμενη στους distinguishers N7 και N6, η οποία είναι ανταγωνιστική απέναντι στις καλύτερες επιθέσεις που έχουν δημοσιευτεί για τον Speck32/64 11 γύρων. Η υπάρχουσα επίθεση του Dinur έχει 2^{46} αξιολογήσεις και αναμένεται να επιτύχει μετά από εξέταση 2^{13} επιλεγμένων ζευγών απλού κειμένου και απόκτησης των αντίστοιχων κρυπτοκειμένων. Η προτεινόμενη επίθεση που μελετάμε αναμένεται να επιτύχει μετά από 2^{38} αξιολογήσεις αν εκτελεστεί σε επεξεργαστή.

6.4.1 Βασική Ιδέα

Η ιδέα είναι να επεκταθεί ο νευρωνικός distinguisher 7 γύρων σε 9 γύρων ετοιμάζοντας μία διαφορική μετάβαση δ→0x0040/0000 που έχει πιθανότητα να είναι επιθυμητή 1/64. Ο 9 γύρων distinguisher επεκτείνεται χωρίς επιπλέον κόστος σε ένα ακόμη γύρο με κρυπτογράφηση των ζευγών P_0, P_1 που κρυπτογραφούνται στην επιθυμητή διαφορά εισροή δ μετά από 1 γύρο Speck κρυπτογράφησης, το οποίο είναι εύκολο γιατί δεν γίνεται κάποια προσθήκη κλειδιού πριν τη πρώτη μη γραμμική επιχείρηση.

Το σήμα από τον distinguisher θα είναι μάλλον αδύναμο. Οπότε ενισχύεται με πιθανολογικά νευρωνικά bits k για να δημιουργηθεί από κάθε ζευγάρι απλού κειμένου ένα κείμενο δομημένο από 2^k που αναμένεται να περάσουν το αρχικό διαφορικό 2 γύρων. Για κάθε δομή απλού κειμένου, αποκρυπτογραφούμε τα τελικά κρυπτοκείμενα με όλα τα τελικά δευτερεύοντα κλειδιά και ταξινομούμε τη κάθε μια αποκρυπτογραφημένη κρυπτογραφική δομή με τους νευρωνικούς distinguishers. Αν το αποτέλεσμα είναι πάνω από ένα κατώφλι c_1 , επιχειρούμε να αποκρυπτογραφήσουμε άλλο ένα γύρο και βαθμολογούμε τα μερικώς αποκρυπτογραφημένα κρυπτοκείμενα χρησιμοποιώντας έναν 6 γύρων νευρωνικό distinguisher. Μία πρόβλεψη κλειδιού επιστρέφεται αν το σκορ που έχουμε ως αποτέλεσμα για αυτή τη δομή ξεπερνά ένα άλλο κατώφλι c_2.

Παράμετροι επίθεσης : Η αρχική διαφορά (0χ211/0/a04) και το σύνολο νευρωνικών bits 14,15,20,21,22,23 δουλεύουν καλά, παρόλο που τα bits 14,15 και 23 δεν είναι τελείως νευρωνικά. Χρησιμοποιούμε c_1=15 , c_2=100 πετυχαίνουμε μία επίθεση με μέσο όρο τα 20 λεπτά υπολογισμών σε ένα μηχάνημα εξοπλισμένο με GTX 1080 κάρτα γραφικών ή 12 ώρες σε έναν απλό υπολογιστή. Στις 100 δοκιμές έχουμε ως εκροή μία πρόβλεψη κλειδιού αφού έχουν επεξεργαστεί κατά μέσο όρο $2^{13.2}$ ζευγών κρυπτοκειμένων. Η ανάκτηση των δύο αληθινών δευτερευόντων κλειδιών ήταν επιτυχής σε 81 περιπτώσεις, το τελικό δευτερεύον κλειδί προβλέφθηκε σωστά σε 99 περιπτώσεις. Στη μία περίπτωση το προτελευταίο δευτερεύον κλειδί ήταν σωστό και η πρόβλεψη για το τελευταίο δευτερεύον κλειδί ήταν λάθος σε ένα bit.

Βελτιωμένη επίθεση: Η βασική ιδέα μπορεί να βελτιωθεί ως εξής:

1. Η υπόθεση ταξινόμησης τυχαίου κλειδιού δεν ευσταθεί όταν πραγματοποιείται μόνο μία επανάληψη δοκιμαστικής αποκρυπτογράφησης , ειδικά σε ‘’ελαφρά‘’ κρυπτογραφήματα. Το χρησιμοποιούμε για να εισάγουμε έναν αλγόριθμο γενικής βελτιστοποίησης.
2. Δεν είναι αποδοτικό να δαπανούμε το ίδιο μέγεθος υπολογισμών σε κάθε κρυπτογραφική δομή. Χρησιμοποιούμε μία μέθοδο για να εστιαστεί η αναζήτηση κλειδιού στις πιο υποσχόμενες κρυπτογραφικές δομές.

Με αυτές τις βελτιώσεις, χτίζεται μία επίθεση που ανακτά τα τελευταία δύο κλειδιά του Speck32/64 11 γύρων με πιθανότητα επιτυχίας 50% από κρυπτοκείμενα ανταποκρινόμενα σε 12800 επιλεγμένα απλά κείμενα σε 8 λεπτά εκτέλεσης σε ένα μονοπύρηνο CPU.

Η *bayesian optimization* είναι μία μέθοδος συχνά χρησιμοποιούμενη για την βελτιστοποίηση συναρτήσεων black box f που είναι ακριβές να αξιολογηθούν. Χρησιμοποιεί προηγούμενη γνώση για την συνάρτηση που είναι να βελτιστοποιηθεί για να κατασκευαστεί ένα πιθανολογικό μοντέλο της συνάρτησης που είναι εύκολο να βελτιστοποιηθεί. Η γνώση για τις παραμέτρους του μοντέλου προστίθεται για να φιλοξενήσει εισροές από αξιολογήσεις συναρτήσεων $f(x_0)$, $f(x_1)$,.., $f(x_n)$. Μία συνάρτηση acquisition χρησιμοποιείται για να αποφασίσει

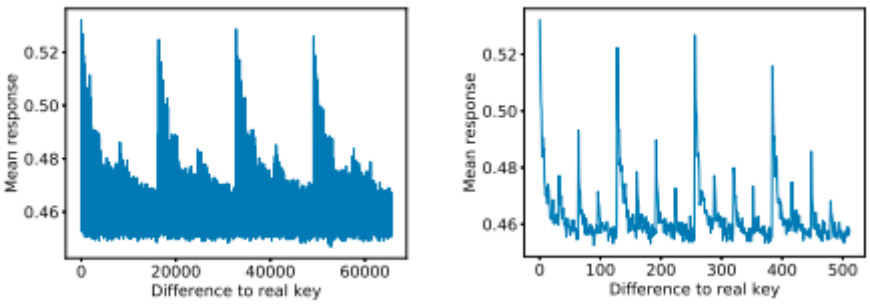
ποια σημεία της συνάρτησης θα προχωρήσουν για να βελτιωθεί όσο γίνεται η γνώση στο μέγιστο. Σε αυτή την έρευνα χρησιμοποιείται τέτοια βελτιστοποίηση για μία αποτελεσματική έρευνα κλειδιού για Speck μειωμένου γύρου. Αυτή η πολιτική μειώνει τον αριθμό των δοκιμαστικών αποκρυπτογραφήσεων που χρησιμοποιεί η επίθεση μας, στο κόστος ενός ακριβού βήματος βελτιστοποίησης. Η βασική ιδέα είναι ότι η πολιτική αναζήτησης κλειδιού είναι ότι η αναμενόμενη απάντηση του distinguisher στην αποκρυπτογράφηση λάθους κλειδιού θα εξαρτηθεί στην δυαδική διαφορά μεταξύ του δοκιμαστικού κλειδιού και πραγματικού κλειδιού. Δοθέντων δοκιμαστικών αποκρυπτογραφήσεων, το βήμα βελτιστοποίησης προσπαθεί να εντοπίσει ένα νέο σύνολο υποθέσεων κλειδιού. Αυτές οι υποθέσεις επιλέγονται έτσι ώστε να μεγιστοποιούν την πιθανότητα των παρατηρηθέντων απαντήσεων των distinguishers.

Υποθέσεις του μοντέλου: Έστω C_0 , C_1 είναι ένα ζεύγος κρυπτογραφημάτων και k το πραγματικό δευτερεύον κλειδί που χρησιμοποιείται στον τελευταίο γύρο κρυπτογράφησης. Έστω $\delta \in F_2^{16}$ και $k' = k \oplus \delta$ είναι το λάθος κλειδί. Η απάντηση του distinguisher D για αποκρυπτογράφηση από το κλειδί k'

$$R_{D,\delta}(C_0, C_1) := D(E_{k'}^{-1}(C_0), E_{k'}^{-1}(C_1)).$$

Το $R_{D,\delta}$ είναι μια τυχαία μεταβλητή που βασίζεται στο δ και προκαλείται από την διανομή του κρυπτογραφικού ζεύγους και υπολογίζει το μέσο μ_δ και την τυπική απόκλιση σ_δ . Αν πάρουμε τη μέση τιμή της απάντησης του distinguisher σε όλα τα στοιχεία της δομής του κρυπτοκειμένου μεγέθους n όπως χρησιμοποιήθηκαν στην επίθεση, ο μέσος όρος αναμένεται να ακολουθεί μία κανονική κατανομή με μέσο μ_δ και τυπική απόκλιση $\sigma_\delta/\sqrt{n}$.

Τυχαιοποίηση λάθους κλειδιού: Υπολογίστηκε η απάντηση λάθος κλειδιού για distinguishers 6 και 7 γύρων για Speck32/64. Για να υπολογίσουμε το r+1 παράχθηκαν 3000 τυχαία κλειδιά και ζεύγη εισροής P_0, P_1 για κάθε δ και κρυπτογραφούμε για r+1 γύρους για να αποκτήσουμε κρυπτοκείμενα C_0, C_1. Ορίζουμε το τελικό δευτερεύον κλειδί για κάθε κρυπτογράφηση με k και εκτελούμε αποκρυπτογράφηση ενός γύρου για να πάρουμε $E_{k\oplus\delta}^{-1}(C_0)$, $E_{k\oplus\delta}^{-1}(C_1)$ και πήραμε το μερικώς αποκρυπτογραφημένο ζεύγος και βαθμολογήθηκε από ένα r γύρων νευρωνικό distinguisher . μ_δ και σ_δ υπολογίστηκαν εμπειρικά στις 3000 δοκιμές. Το προφίλ για έξι γύρους φαίνεται παρακάτω. Η δομή είναι μη τυχαία και το σχήμα των καμπυλών για σ_δ είναι παρόμοια και για τους 6 γύρους.



Παραπάνω φαίνεται η μ_δ για Speck32/64 8 γύρων και νευρωνικό distinguisher 7 γύρων για 3000 ζεύγη.

Χρήση του προφίλ του λάθος κλειδιού για αναζήτηση κλειδιού: Δοθέντων των συμπερασμάτων και παρατηρήσεων της απάντησης του distinguisher r_0 , r_1,…, r_{n-1} για κλειδιά $k_0, k_1, .., k_{n-1}$ μπορούμε να δούμε τα r_i ως τιμές αποκτημένες από μία n διαστάσεων κανονική κατανομή. Οι παράμετροι αυτής της κατανομής βασίζεται στις δυαδικές διαφορές του k_i και του πραγματικού τελευταίου δευτερεύοντος κλειδιού ειδικά $\mu_{k\oplus k}$ και $\sigma_{k\oplus k}$. Ελαχιστοποιώντας την

ευκλείδεια απόσταση βαρών $\sum_{i=0}^{n-1}(m_i-\mu_{k\oplus k_i})^2/\sigma^2_{k\oplus k_i}$ μεγιστοποιείται η πιθανολογική πυκνότητα των τιμών. Παρακάτω απεικονίζεται ο αλγόριθμος.

Algorithm 4 BayesianKeySearch: efficiently find a list of plausible key candidates given a ciphertext structure satisfying the initial differential of our attack.

Require: Ciphertext structure $C = C_0, \dots C_{m-1}$, neural distinguisher N, number of candidates to be generated n, number of iterations l.

$S := \{k_0, k_1, \dots, k_{n-1}\} \leftarrow$ choose at random without replacement from the set of all subkey candidates.
$L \leftarrow \{\}$
for $j \in \{0, 1, \dots, l-1\}$: **do**
  $P_{i,k} \leftarrow Decrypt(C_i, k)$ for all $i \in \{0, 1, \dots, m-1\}$, $k \in S$.
  $v_{i,k} \leftarrow N(P_{i,k})$ for all i,k
  $w_{i,k} \leftarrow \log_2(v_{i,k}/(1-v_{i,k}))$ for all $i \in \{0, \dots, m-1\}, k \in S$
  $w_k \leftarrow \sum_{i=1}^{n} v_{i,k}$for all$k \in S$
  $L \leftarrow L|||[(k, w_k)$ for $k \in S]$
  $m_k \leftarrow \sum_{i=0}^{n-1} v_{i,k}/n$ for $k \in \{k_0, \dots, k_{n-1}\}$
  $\lambda_k \leftarrow \sum_{i=0}^{n-1}(m_{k_i} - \mu_{k_i \oplus k})^2/\sigma^2_{k_i \oplus k}$ for $k \in \{0, 1, \dots, 2^{16}-1\}$:
  $S \leftarrow \text{argsort}_k(\lambda)[0 : n-1]$
end for
return L

Όλες οι δοκιμές των κλειδιών και το σκορ τους w_k αποθηκεύονται. Τα κλειδιά με σκορ πάνω από ένα κατώφλι c_1 επαναλαμβάνουν την διαδικασία για ένα ακόμη γύρο. Ο αλγόριθμος 4 χρησιμοποιείται με έναν 6 γύρων νευρωνικό distinguisher και σχετίζεται με το προφίλ λάθος κλειδιού. Αν ένα από τα υποψήφια κλειδιά που προκύπτουν έχει βαθμολογία πάνω από ένα κατώφλι c_2 , τερματίζεται η αναζήτηση , αλλά η επεξεργασία του τρέχοντος κόμβου αναζήτησης τελειώνει πριν το καλύτερο εβρισκόμενο ζεύγος δευτερευόντων κλειδιών για τους τελευταίους δύο γύρους επιστραφεί.

Πριν δοθεί ως αποτέλεσμα ένα κλειδί, εκτελούμε μία μικρή έρευνα επαλήθευσης με ακτίνα 2 γύρω από τα δύο καλύτερα υποψήφια που είναι τα τρέχοντα καλύτερα. Αυτό απομακρύνει τα λάθη των bit στην πρόβλεψη κλειδιού. Αν η έρευνα επαλήθευσης παρουσιάσει μία βελτίωση, επαναλαμβάνεται με τις νέες προβλέψεις κλειδιού.

Δοθέντων t κρυπτογραφικών δομών, ο αλγόριθμος δοκιμάζεται πρώτα σε κάθε δομή, αν δεν βρεθεί λύση συνεχίζεται για ένα καθορισμένο αριθμό επαναλήψεων πριν επιστρέψει τα ζεύγη των δευτερευόντων κλειδιών με την υψηλότερη βαθμολογία στους τελευταίους γύρους. Σε αυτές τις επαναλήψεις επιλέγουμε σε ποιες κρυπτογραφικές δομές θα επενδυθεί ο προϋπολογισμός . Το αντιμετωπίζουμε ως ένα πρόβλημα *multi –armed bandit* και το λύνουμε χρησιμοποιώντας μία κοινή μέθοδο εξερεύνησης – εκμετάλλευσης, την Upper Confidence Bounds (UCB). Η σειρά που θα ελεγχούν οι δομές σε αυτή τη φάση εξαρτάται από το υψηλότερο αποτέλεσμα των distinguishers στην τελευταία έρευνα αναζήτησης κλειδιού και στον αριθμό επισκέψεων στην αναζήτηση. Ορίζουμε ως w^i_{max} το υψηλότερο βαθμό distinguishers για την ith κρυπτογραφική δομή , n_i τον αριθμό των προηγούμενων επαναλήψεων στις οποίες η ith δομή επιλέχθηκε και j τον αριθμό της τρέχουσας επανάληψης. Υπολογίζουμε μία βαθμολογία προταιρεότητας :

$$s_i := w^i_{\max} + \alpha \cdot \sqrt{\log_2(j)/n_i}$$

και επιλέγεται η κρυπτογραφική δομή με την υψηλότερη βαθμολογία για περαιτέρω επεξεργασία. Το καλύτερο αποτέλεσμα ανανεώνεται μετά το τέλος της επανάληψης. Ρυθμίζουμε a στο $\sqrt{n_c}$ όπου n_c είναι οι διαθέσιμες κρυπτογραφικές δομές.

Αποτελέσματα: Στις δοκιμές που παρουσιάστηκαν, χρησιμοποιήθηκαν 100 δομές κρυπτογραφικές από 64 κρυπτογραφήσεις επιλεγμένων ζευγών απλών κειμένων, c1=5, c2=10, UCB προϋπόθεση α=10 και για την πολιτική Bayesian l=5 αριθμός υποψηφίων n=32 και budget για την επανάληψη it=500. Δοθέντων 100 κρυπτογραφικών δομών σε 8 λεπτά παράγεται κατά μέσο όρο ως εκροή μία πρόβλεψη κλειδιού. Δεν είναι πάντα σωστή αυτή η πρόβλεψη αλλά αν είναι έτσι ξεχωρίζεται από τα επιστρεφόμενα αποτελέσματα. Η πολιτική έρευνας κλειδιού προσπαθεί με αυτές τις ρυθμίσεις μόνο 160 κλειδιά ενώ επεξεργάζεται μία κρυπτογραφική κατασκευή.

Μία πρόβλεψη θεωρείται σωστή αν το κλειδί τελευταίου γύρου προβλέφθηκε σωστά και αν αυτό του δεύτερου γύρου είναι σε απόσταση σφυρηλάτησης μέγιστη δύο του πραγματικού κλειδιού. Υπό αυτές τις συνθήκες, η επίθεση ήταν επιτυχής σε 521 από 1000 δοκιμές.

6.5 Πείραμα Real Differences

Θα παρουσιαστεί ένα κρυπτογραφικό πείραμα στο οποίο η διαφορική κατανομή τυχαία και πραγματικοί είναι ίδιες. Θα αποδειχτεί ότι οι νευρωνικοί distinguishers είναι αποτελεσματικοί.

Αρχικά, 10^6 δείγματα πάρθηκαν από την κανονική κατανομή για τα D5,D6,D7 και D8 σκοπούς. Για τα μισά από αυτά : για εκροή ένα ζεύγος κρυπτοκειμένων C= $(C_0,C_1) \in F_2^{2b}$ παράγεται μία τιμή K$\in F_2^{2b}$. Αυτή η τιμή έγινε δυαδική προσθήκη και στα δύο κρυπτοκείμενα και παράχθηκε :

$\tilde{C} = (C_0 \oplus K, C_1 \oplus K).$

Αυτά τα δείγματα ,αφού επεξεργαστούν με αυτό τον τρόπο, τα αποτελέσματα περνάν στους νευρωνικούς distinguishers για ταξινόμηση ως τυχαία ή όχι.

Πρώτα υπολογίζουμε : $A_{rand} := 2^{64}$ DP(ΔC) ,όπου DP(ΔC) είναι η διαφορική πιθανότητα να παρατηρήσουμε την διαφορά εκροής του ζεύγους C , όπως δίνεται από το μοντέλο Marcov. Έπειτα, ορίζουμε ως D_{mid} το σύνολο των πιθανών διαφορών 3 γύρων , με P(δ) τη πιθανότητα να παρατηρηθεί η διαφορά 3 γύρου δ και

N_δ (C) ο αριθμός των λύσεων για τα δύο τελευταία δευτερεύοντα κλειδιά που αποκρυπτογράφησαν το C με στη διαφορά δ του γύρου 3 υπολογίζουμε

$A_{\text{real}} := 2^{32} \cdot \sum_{\delta \in \mathcal{D}_{\text{mid}}} P(\delta) \cdot N_\delta(C).$

Το C είναι αληθές αν $A_{real} > A_{rand}$, και τυχαίο αλλιώς.

Αποτελέσματα : Τα καλύτερα δίκτυα επέλυσαν τις διαφορές καλύτερα από την τυχαία πρόβλεψη χωρίς να έχουν εκπαιδευτεί. Στον πίνακα φαίνονται οι λεπτομέρειες :

Nr	Distinguisher	Accuracy
5	N5	$0.707 \pm 9.10 \cdot 10^{-4}$
6	N6	$0.606 \pm 9.77 \cdot 10^{-4}$
7	N7	$0.551 \pm 9.95 \cdot 10^{-4}$
8	N8	$0.507 \pm 1.00 \cdot 10^{-3}$
5	Search	$0.810 \pm 7.84 \cdot 10^{-3}$
5	N5 retrained	$0.762 \pm 8.51 \cdot 10^{-4}$

Η χρήση των νευρωνικών distinguishers ως εργαλείο αναζήτησης καθιστά εύκολη την εύρεση παραδειγμάτων ζευγών κρυπτοκειμένων με σχετικά μεγάλη πιθανότητα διαφορών με μικρή πιθανότητα εμφάνισης στην κατανομή του μειωμένου Speck.

6.6 Συμπεράσματα

Σκοπός της έρευνας που παρουσιάστηκε σε αυτό το κεφάλαιο ήταν να δοκιμαστεί το αν τα νευρωνικά δίκτυα μπορούν να χρησιμοποιηθούν για να αναπτύξουν στατιστικές δοκιμές που αποτελεσματικά εκμεταλλεύονται διαφορικές ιδιότητες ενός συμμετρικού αρχικού σχήματος ,που έχει προηγουμένως αποδυναμωθεί με επαναλήψεις, έτσι ώστε οι επιθέσεις να γίνουν σε μικρότερο όγκο δεδομένων. Στην περίπτωση που μελετήθηκε, οι distinguishers πρόσφεραν καλύτερη ακρίβεια, χρησιμοποίησαν λιγότερη μνήμη, ακόμη και αν η ταχύτητα είναι χαμηλότερη συγκρινόμενη με την απλή αναζήτηση μνήμης που απαιτείται από έναν προϋπολογισμένο πίνακα διανομής διαφοράς. Όλη αυτή η γνώση για την διαφορική διανομή του Speck μειωμένων επαναλήψεων μπορεί να εξαχθεί από κάποια εκατομμύρια παραδείγματα μεθόδων black box[9].

Ο χρόνος που χρειάστηκε για την εκπαίδευση του δικτύου μετριέται σε λεπτά αν υπάρχει μία γρήγορη κάρτα γραφικών. Οι distinguishers έχουν πολλές νέες ιδιότητες , όπως την ικανότητα να βρίσκουν διαφορές μεταξύ ζευγών στην ίδια κλάση διαφοράς.

Η παρούσα έρευνα φυσικά επιδέχεται βελτίωση. Θα μπορούσε το μοντέλο να έχει περισσότερη γνώση για το κρυπτογράφημα ή ο ερευνητής να μπορεί να εξάγει ευκολότερα γνώση από ένα εκπαιδευμένο μοντέλο. Μικρές βελτιώσεις μπορούν να γίνουν στην αρχιτεκτονική και τις ρυθμίσεις. Οι συγκεκριμένοι ερευνητές θεωρούν ότι οι μέθοδοι μηχανικής εκμάθησης δεν θα υποσκελίσουν την παραδοσιακή κρυπτανάλυση , αλλά τα νευρωνικά δίκτυα μπορούν να μάθουν να κρυπταναλύουν σε ένα ενδιαφέρον επίπεδο για τους κρυπτογράφους και να είναι μία σημαντική προσθήκη στην όλη έρευνα.

ΚΕΦΑΛΑΙΟ 7ο : ΣΥΜΠΕΡΑΣΜΑΤΑ - ΤΟ ΜΕΛΛΟΝ ΤΗΣ ΚΡΥΠΤΑΝΑΛΥΣΗΣ

ΤΕΧΝΗΤΗ ΝΟΗΜΟΣΥΝΗ: Ο όρος τεχνητή νοημοσύνη αναφέρεται στον κλάδο της πληροφορικής ο οποίος ασχολείται με τη σχεδίαση και την υλοποίηση υπολογιστικών συστημάτων που μιμούνται στοιχεία της ανθρώπινης συμπεριφοράς τα οποία υπονοούν έστω και στοιχειώδη ευφυΐα: μάθηση, προσαρμοστικότητα, εξαγωγή συμπερασμάτων, κατανόηση από συμφραζόμενα, επίλυση προβλημάτων κλπ. Ο Τζον Μακάρθι όρισε τον τομέα αυτόν ως «επιστήμη και μεθοδολογία της δημιουργίας νοημόνων μηχανών».
Πλέον η τεχνητή νοημοσύνη είναι μέρος της καθημερινότητας μας. Στην πιο απλή της μορφή, όλοι έχουμε από ένα κινητό τηλέφωνο με το οποίο διεκπεραιώνουμε διάφορες υποχρεώσεις, επικοινωνούμε με πολλούς τρόπους και μας ακούει κυριολεκτικά , αλληλοεπιδρά μαζί μας. Έχοντας λοιπόν την τεχνολογία τόσο στην ζωή μας είναι λογικό η κρυπτογράφηση να γίνεται με χρήση αλγορίθμων, πολύπλοκων υπολογιστικών συστημάτων, τεχνητής νοημοσύνης και μηχανικής εκμάθησης γενικότερα. Η εποχή που η κρυπτογράφηση και η κρυπτανάλυση γινόταν με το χέρι και απλά τη σκέψη των ανθρώπων έχει περάσει ανεπιστρεπτί. Η ταχύτητα με την οποία γίνεται η προσπέλαση δεδομένων και η εξαγωγή συμπερασμάτων μέσω της τεχνητής νοημοσύνης δεν μπορεί να συγκριθεί με τις παραδοσιακές μεθόδους. Εφόσον οι πληροφορίες και τα δεδομένα κυκλοφορούν, επεξεργάζονται και αποθηκεύονται μέσω τεχνητής νοημοσύνης είναι λογικό να κρυπτασφαλίζονται και αντίστοιχα να κρυπταναλύονται με τέτοιες μεθόδους. Οι εργασίες γίνονται μέσω αυτών και οι μηχανές δεν έχουν αντικαταστήσει τον άνθρωπο φυσικά, αλλά βοηθούν σε μεγάλο βαθμό τον άνθρωπο.

Ακριβώς αυτό είναι και η κρυπτανάλυση με μεθόδους τεχνητής νοημοσύνης . Οι άνθρωποι κρίνουν το τι θα κρυπτογραφήσουν/κρυπταναλύσουν και με ποιες μεθόδους, αλλά δημιουργούν αλγόριθμους που εκτελούν αυτές τις εργασίες. Στην παρούσα διατριβή παρουσιάστηκαν διάφορες μέθοδοι, συγκρινόμενες μεταξύ τους και για διαφορετικές περιπτώσεις κρυπτογραφημάτων, από μελέτες και πειράματα που ήδη έχουν παρουσιαστεί στον τομέα.

Συνεχώς μελετώνται νέες μέθοδοι για κρυπτογράφηση και συνεπώς κρυπτανάλυσης , καθώς η κρυπτανάλυση προάγει και συνεχώς ‘’πιέζει’’ τον τομέα της κρυπτογραφίας να βελτιωθεί, εντοπίζοντας τα αδύναμα σημεία κάθε κρυπτοσυστήματος. Υπάρχουν ακόμη βέβαια κρυπτοσυστήματα που δεν έχει επιτευχθεί η πλήρης κρυπτανάλυση τους, όπως το Speck, το οποίο αναλύθηκε στο 6ο κεφάλαιο.

<u>Το μέλλον στην Κρυπτανάλυση.</u>

Τα Τεχνητά Νευρωνικά Δίκτυα είναι γενικότερα η νέα τάση στον τομέα της τεχνητής νοημοσύνης, και κατά συνέπεια και στην κρυπτανάλυση. Προσφέρουν παράλληλη επεξεργασία δεδομένων και είναι ικανά να επεξεργαστούν μεγάλες ποσότητες δεδομένων σε σύντομο χρονικό διάστημα. Είναι ευέλικτα και προσαρμόζονται εύκολα σε διάφορες περιπτώσεις. Υπάρχει συνεχής πρόοδος στον τομέα και εξελίσσεται ραγδαία κατακτώντας όλο και περισσότερους στόχους.

Τα ΤΝΔ μιμούνται το ανθρώπινο νευρικό σύστημα. Υπάρχει γενικότερα μία τάση, μία στροφή, στις επιστημονικές μεθόδους να μιμούνται τομείς της βιολογίας . Κρυπτογραφία DNA για παράδειγμα, είναι η νέα τάση, αν και βιομετρικές μέθοδοι χρησιμοποιούνται χρόνια στον τομέα της ασφάλειας. Συνεπώς, τα ΤΝΔ που είναι ένα κομμάτι αυτής της τάσης είναι σίγουρα το μέλλον στην κρυπτανάλυση.

ΕΠΕΞΗΓΗΣΕΙΣ

1. Internet of Things (IoT) : Το Διαδίκτυο των πραγμάτων (Internet of things) αποτελεί το δίκτυο επικοινωνίας πληθώρας συσκευών, οικιακών συσκευών, αυτοκινήτων καθώς και κάθε αντικειμένου που ενσωματώνει ηλεκτρονικά μέσα, λογισμικό, αισθητήρες και συνδεσιμότητα σε δίκτυο ώστε να επιτρέπεται η σύνδεση και η ανταλλαγή δεδομένων. Απλούστερα, η φιλοσοφία του IoT είναι η σύνδεση όλων των ηλεκτρονικών συσκευών μεταξύ τους (τοπικό δίκτυο) ή με δυνατότητα σύνδεσης στο διαδίκτυο (παγκόσμιο ιστό). Η έννοια "Things" (πράγματα) δεν είναι αυστηρά συνδεδεμένη με ορισμένα προϊόντα. Αναφέρεται σε μία ευρεία ποικιλία συσκευών εντελώς διαφορετικά μεταξύ τους, όπως για παράδειγμα αυτοκίνητα με ενσωματωμένους αισθητήρες, κάμερες, κλιματιστικά, φώτα, συστήματα ασφαλείας, smartwatches ακόμα και αυτοκίνητα των οποίων οι περίπλοκοι αισθητήρες εντοπίζουν αντικείμενα στην πορεία τους. Βασικό χαρακτηριστικό όλων είναι η σύνδεση μεταξύ τους με απώτερο σκοπό την δυνατότητα του χρήστη να τα ελέγχει από έναν υπολογιστή ή κινητό. Ο όρος Internet of Things αποδόθηκε την δεκαετία του 1990 από τον Kevin Ashton.
2. Distinguisher: Στα ελληνικά μπορεί να αποδοθεί ως ‘’ ταξινομητής’’ ή ‘’ διακριτής’’, δεν υπάρχει στην ελληνική ορολογία. Ουσιαστικά είναι μία επίθεση που ξεχωρίζει το κρυπτοκείμενο από τυχαία δεδομένα.
3. ARX : Add Rotate Xor Κρυπτογράφημα.
4. Power analysis : Η ανάλυση ισχύος είναι μια μορφή επίθεσης πλάγιου καναλιού στην οποία ο εισβολέας μελετά την κατανάλωση ενέργειας μιας κρυπτογραφικής συσκευής υλικού. Αυτές οι επιθέσεις βασίζονται σε βασικές φυσικές ιδιότητες της συσκευής: οι συσκευές ημιαγωγών διέπονται από τους νόμους της φυσικής, οι οποίοι υπαγορεύουν ότι οι αλλαγές στις τάσεις εντός της συσκευής απαιτούν πολύ μικρές κινήσεις ηλεκτρικών φορτίων (ρεύματα).Με τη μέτρηση αυτών των ρευμάτων είναι δυνατόν να πάρετε μια μικρή ποσότητα πληροφοριών σχετικά με τα δεδομένα που χειρίζονται.
5. Residual tower: Ένα υπολειπόμενο νευρικό δίκτυο (ResNet) είναι ένα τεχνητό νευρικό δίκτυο (ANN) ενός είδους που βασίζεται σε κατασκευές γνωστές από πυραμιδικά κύτταρα στον εγκεφαλικό φλοιό . Τα υπολειπόμενα νευρωνικά δίκτυα το κάνουν χρησιμοποιώντας παραλείψεις συνδέσεων ή συντομεύσεις για να ξεπεράσουν κάποια επίπεδα. Τα τυπικά μοντέλα ResNet εφαρμόζονται με παραλείψεις διπλού ή τριπλού επιπέδου που περιέχουν μη γραμμικότητες (ReLU) και ομαλοποίηση παρτίδων στο μεταξύ.
6. Convolutional : Στη βαθιά μάθηση , ένα συνελικτικό νευρικό δίκτυο (CNN ή ConvNet) είναι μια κατηγορία βαθιών νευρωνικών δικτύων , τα οποία συνήθως χρησιμοποιούνται για την ανάλυση οπτικών εικόνων. [1] Είναι επίσης γνωστοί ως τεχνητά νευρωνικά δίκτυα μετατόπισης μεταβλητών ή διαστημικών αμετάβλητων (SIANN), με βάση την αρχιτεκτονική κοινόχρηστου βάρους των πυρήνων συνέλιξης που μετατοπίζουν χαρακτηριστικά εισόδου και παρέχουν ισοδύναμες αποκρίσεις μετάφρασης .
7. Bit slice : Τεμαχισμός bit, είναι μια τεχνική για την κατασκευή ενός επεξεργαστή από ενότητες επεξεργαστών μικρότερου πλάτους bit, με σκοπό την αύξηση του μήκους της λέξης, θεωρητικά για να φτιάξουμε έναν αυθαίρετο επεξεργαστή n-bit. Κάθε μία από αυτές τις λειτουργικές μονάδες επεξεργάζεται ένα πεδίο bit ή "slice" ενός τελεστή.
8. Black box : Στην επιστήμη, την πληροφορική και τη μηχανική, ένα μαύρο κουτί είναι μια συσκευή, σύστημα ή αντικείμενο που μπορεί να προβληθεί ως προς τις εισόδους και τις εξόδους του, χωρίς καμία γνώση των εσωτερικών του λειτουργιών. Η εφαρμογή του είναι αδιαφανής ή «μαύρη». Σχεδόν οτιδήποτε μπορεί να αναφέρεται ως μαύρο κουτί: τρανζίστορ, αλγόριθμος ή ακόμα και ανθρώπινος εγκέφαλος.

ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Evolutionary Computation Based Cryptanalysis – E.C. Laskari, G.C. Meletiou, Y.C. Stamatiou, M.N. Vrahatis
2. Cryptography and Cryptanalysis through Computational Intelligence - E.C. Laskari, G.C. Meletiou, Y.C. Stamatiou, M.N. Vrahatis
3. Improving Attacks on round-reduced Speck32/64 using deep learning- Aron Gohr
4. Wikipedia
5. Various approaches towards cryptanalysis – Shaligram Prajapat, Ramjeevan Thakur
6. Neural Cryptanalysis of classical ciphers – Riccardo Focardi, Flaminia L.Luccio
7. Applications of machine learning in cryptography: a survey – Mohammed M.Alani