ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΙΑΤΡΙΚΗ

ΓΕΝΙΚΕΥΜΕΝΕΣ ΑΚΟΛΟΥΘΙΕΣ FIBONACCI ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

Αθανάσιος Παγιαβλάς

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ
Επιβλέποντες

Μαρία Αδάμ
Αναπληρώτρια Καθηγήτρια

Γεώργιος Σπαθούλας
Μέλος ΕΔΙΠ

Λαμία, Σεπτέμβριος 2017

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ
ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΜΕ ΕΦΑΡΜΟΓΕΣ ΣΤΗ ΒΙΟΙΑΤΡΙΚΗ

ΓΕΝΙΚΕΥΜΕΝΕΣ ΑΚΟΛΟΥΘΙΕΣ FIBONACCI ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

Αθανάσιος Παγιαβλάς

ΠΤΥΧΙΑΚΗ ΕΡΓΑΣΙΑ

Επιβλέποντες

Μαρία Αδάμ

Αναπληρώτρια Καθηγήτρια

Σπαθούλας Γεώργιος

Μέλος ΕΔΙΠ

Λαμία, Σεπτέμβριος 2017

Με ατομική μου ευθύνη και γνωρίζοντας τις κυρώσεις [1], που προβλέπονται από της διατάξεις της παρ. 6 του άρθρου 22 του Ν. 1599/1986, δηλώνω ότι:

1. *Δεν παραθέτω κομμάτια βιβλίων ή άρθρων ή εργασιών άλλων αυτολεξεί* ***χωρίς να τα περικλείω σε εισαγωγικά*** *και χωρίς να αναφέρω το συγγραφέα, τη χρονολογία, τη σελίδα. Η αυτολεξεί παράθεση χωρίς εισαγωγικά χωρίς αναφορά στην πηγή, είναι λογοκλοπή. Πέραν της αυτολεξεί παράθεσης, λογοκλοπή θεωρείται και η παράφραση εδαφίων από έργα άλλων, συμπεριλαμβανομένων και έργων συμφοιτητών μου, καθώς και η παράθεση στοιχείων που άλλοι συνέλεξαν ή επεξεργάσθηκαν, χωρίς αναφορά στην πηγή. Αναφέρω πάντοτε με πληρότητα την πηγή κάτω από τον πίνακα ή σχέδιο, όπως στα παραθέματα.*

2. *Δέχομαι ότι η αυτολεξεί* ***παράθεση χωρίς εισαγωγικά****, ακόμα κι αν συνοδεύεται από αναφορά στην πηγή σε κάποιο άλλο σημείο του κειμένου ή στο τέλος του, είναι αντιγραφή. Η αναφορά στην πηγή στο τέλος π.χ. μιας παραγράφου ή μιας σελίδας, δεν δικαιολογεί συρραφή εδαφίων έργου άλλου συγγραφέα, έστω και παραφρασμένων, και παρουσίασή τους ως δική μου εργασία.*

3. *Δέχομαι ότι υπάρχει επίσης περιορισμός στο μέγεθος και στη συχνότητα των παραθεμάτων που μπορώ να εντάξω στην εργασία μου εντός εισαγωγικών. Κάθε μεγάλο παράθεμα (π.χ. σε πίνακα ή πλαίσιο, κλπ), προϋποθέτει ειδικές ρυθμίσεις, και όταν δημοσιεύεται προϋποθέτει την άδεια του συγγραφέα ή του εκδότη. Το ίδιο και οι πίνακες και τα σχέδια*

4. *Δέχομαι όλες τις συνέπειες σε περίπτωση λογοκλοπής ή αντιγραφής.*

Ημερομηνία: ……/…../20……

Ο – Η Δηλ.

(Υπογραφή)

(1) «Όποιος εν γνώσει του δηλώνει ψευδή γεγονότα ή αρνείται ή αποκρύπτει τα αληθινά με έγγραφη υπεύθυνη δήλωση του άρθρου 8 παρ. 4 Ν. 1599/1986 τιμωρείται με φυλάκιση τουλάχιστον τριών μηνών. Εάν ο υπαίτιος αυτών των πράξεων σκόπευε να προσπορίσει στον εαυτόν του ή σε άλλον περιουσιακό όφελος βλάπτοντας τρίτον ή σκόπευε να βλάψει άλλον, τιμωρείται με κάθειρξη μέχρι 10 ετών.

ΓΕΝΙΚΕΥΜΕΝΕΣ ΑΚΟΛΟΥΘΙΕΣ FIBONACCI ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΣΤΗΝ ΚΡΥΠΤΟΓΡΑΦΙΑ

Αθανάσιος Παγιαβλάς

Τριμελής Επιτροπή:

Μαρία Αδάμ, Αναπληρώτρια Καθηγήτρια, ΠΕΒ

Γεώργιος Σπαθούλας, Μέλος ΕΔΙΠ, ΠΕΒ

Αθανάσιος Κακαρούντας, Επίκουρος Καθηγητής, ΠΕΒ

ΕΥΧΑΡΙΣΤΙΕΣ

Η παρούσα πτυχιακή πραγματοποιήθηκε στο Τμήμα Πληροφορικής με Εφαρμογές στη Βιοϊατρική του Πανεπιστημίου Θεσσαλίας.

Έχοντας ολοκληρώσει την παρούσα πτυχιακή θα ήθελα να ευχαριστήσω θερμά:

Τους επιβλέποντες καθηγητές μου κα Μαρία Αδάμ και κ. Γεώργιο Σπαθούλα για τη συνεχή υποστήριξη και ενθάρρυνση κατά τη διάρκεια της εκπόνησης της παρούσας πτυχιακής εργασίας, όπως επίσης και για την πολύτιμη καθοδήγηση και βοήθεια στην επίλυση διαφόρων θεμάτων.

Θα ήθελα να ευχαριστήσω τον κ. Αθανάσιο Κακαρούντα για τη συμμετοχή του στην Εξεταστική Επιτροπή, διαβεβαιώνοντας τον ότι οι παρατηρήσεις του θα ληφθούν σοβαρά υπ' όψιν και θα ενσωματωθούν στο τελικό κείμενο.

Επίσης θα ήθελα να απευθύνω τις ευχαριστίες μου στην οικογένεια μου, η οποία με στήριξε ποικιλοτρόπως και υλικά και ηθικά, καθ' όλη τη διάρκεια των σπουδών μου.

Αθανάσιος Παγιαβλάς

Περιεχόμενα

Εισαγωγή

Από αρχαιοτάτους χρόνους η επικοινωνία ήταν μια από τις σημαντικότερες λειτουργίες για την ανάπτυξη μίας κοινωνίας. Λόγω των διαφορετικών πολιτισμών που υπήρχαν, η ανάγκη για μυστικότητα στον γραπτό λόγο ήταν απαραίτητη, αποτρέποντας τρίτους να παρακολουθήσουν την επικοινωνία τους και να μάθουν τα μυστικά τους, με αποτέλεσμα να αναπτυχθεί η ιδέα της κρυπτογραφίας. Ο ρόλος της στην εξέλιξη της ανθρωπότητας είναι αρκετά σημαντικός. Η κρυπτογραφία είναι ο ένας κλάδος της κρυπτολογίας, ο άλλος είναι η κρυπτανάλυση. Οι Menzes, van Oorschot και Vanstone ορίζουν την κρυπτογραφία ως τη μελέτη μαθηματικών τεχνικών που σχετίζονται με θέματα της ασφάλειας πληροφοριών, η κρυπτογραφία είναι ένας από τους τρόπους με τους οποίους μπορούμε να πετύχουμε πληροφοριακή ασφάλεια [19]. Ενώ το RFC ορίζει την κρυπτογράφηση ως τη μαθηματική επιστήμη που αναφέρεται στο μετασχηματισμό δεδομένων, ώστε να εμποδιστούν ανεντόπιστες τροποποιήσεις, να εμποδιστεί η μη εξουσιοδοτημένη χρήση τους ή να επιτευχθεί κάποιος άλλος στόχος της ασφάλειας πληροφοριών [20]. Η κρυπτογραφία χωρίζεται σε 3 μεγάλες χρονικές περιόδους μέσα στις οποίες δημιουργήθηκαν σημαντικοί κρυπταλγόριθμοι (1900 π. Χ. -1900 μ.Χ., 1900 μ. Χ. -1950 μ.Χ., 1950 μ.Χ.- σημέρα) [21,22]. Την πρώτη περίοδο αναπτύχθηκαν αρκετοί αλγόριθμοι και μέθοδοι κρυπτογράφησης οι οποίοι χωρίζονται σε δυο κατηγορίες απλής αντικατάστασης και αναδιάταξης-μετάθεσης γραμμάτων. Εκείνη την περίοδο οι Σπαρτιάτες εφηύραν μια κρυπτοκατασκευή (Σκυτάλη) [23] και τότε δημιουργήθηκε ο αλγόριθμος του Καίσαρα. Την δεύτερη περίοδο, λόγω των παγκοσμίων πολέμων, η επιστήμη της κρυπτογραφίας αναπτύχθηκε αρκετά μέσα σε λίγα χρόνια και δημιουργήθηκαν σημαντικοί κρυπταλγόριθμοι και μηχανές, όπως ο αλγόριθμος One time Pad ή Vernam [35] και η μηχανή Enigma [36] κ.α.

Τα τελευταία χρόνια, με τη ραγδαία εξέλιξη της τεχνολογίας, δημιουργούνται νέες ανάγκες σχετικά με την ασφάλεια και την ιδιωτικότητα. Για να καλυφθούν αυτές οι ανάγκες συνεχίζει να αναπτύσσεται μία πληθώρα τεχνικών μυστικής επικοινωνίας,

που εντάσσονται στις περιοχές της κρυπτογραφίας και στεγανογραφίας, κ.α. Ένα σημαντικό είδος πληροφορίας είναι οι ψηφιακές εικόνες. Στο συγκεκριμένο είδος πληροφορίας πολλές μέθοδοι κρυπτογραφίας βασίζονται στην αναδιάταξη των pixel της εικόνας. Η πρώτη από αυτές δημιουργήθηκε από τον Arnold [24]. Αργότερα οι Ma και Qiu ανέπτυξαν ένα κρυπτοσύστημα χρησιμοποιώντας τη γενική μέθοδο cat map [25]. Το 2004 αναπτύχθηκε από τους Kong και Dan ένας καινούριος anti-Arnold αλγόριθμος [26]. Οι Hong και Zou επέκτειναν τον αλγόριθμο από 2D σε 3D και μελέτησαν την περιοδικότητα του Arnold [27]. Ο Wang μελέτησε την περιοδικότητα του μετασχηματισμού αναδιάταξης δισδιάστατου τυχαίου πίνακα και τον χρησιμοποιήσε για την απόκρυψη εικόνας [28]. Το 2006 δόθηκε μια νέα τεχνολογία αναδιάταξης εικόνας βασισμένη στη συμμετρία του μετασχηματισμού Arnold [29]. Ο Minati Mishra και άλλοι στις δημοσιεύσεις τους επέκτειναν τη μέθοδο αυτή και γενίκευσαν το μετασχηματισμό Arnold για να αυξήσουν την ασφάλεια της ανακατεμμένης εικόνας [30, 31]. Όταν κάποιοι είχαν επικεντρωθεί στο μετασχηματισμό Arnold, η ομάδα του Qi παρουσίασαν μια νέα μέθοδο μετασχηματισμού και τις εφαρμογές της [32], η οποία αργότερα επεκτάθηκε από τον Zou, ο οποίος χρησιμοποίησε αριθμούς Fibonacci και Fibonacci μετασχηματισμό για την αναδιάταξη της εικόνας [33, 34]. Ο Li-Ping Shao και λοιποί μελέτησαν τη δισδιάστατη τριγωνική απεικόνιση και τις εφαρμογές της στην αναδιάταξη ορθογώνιας εικόνας [11]. Αργότερα δημιουργήθηκε μια μέθοδος κρυπτογράφησης εικόνας χρησιμοποιώντας Fibonacci – Lucas μετασχηματισμό [9].

Στην παρούσα πτυχιακή παρουσιάζονται αλγόριθμοι κρυπτογράφησης τετραγωνικών και μη τετραγωνικών πινάκων με τη χρήση γενικευμένων πινάκων Fibonacci και τον κρυπταλγόριθμο του Hill. Η διαφορά με τις μέχρι σήμερα μεθόδους είναι ότι χρησιμοποιούνται γενικευμένοι πίνακες Fibonacci n-διαστάσεων, οι οποίοι έχουν βάρη διαφορετικά της μονάδας.

Συγκεκριμένα, στο πρώτο κεφάλαιο παρουσιάζονται κάποιες βασικές έννοιες, θεωρήματα και παρατηρήσεις για τα θέματα που προαναφέρθηκαν με σκοπό την κατανόηση του γενικού πλαισίου της παρούσας πτυχιακής.

Στο δεύτερο κεφάλαιο παρουσιάζονται αναλυτικά οι αλγόριθμοι που δημιουργήθηκαν για την κρυπτογράφηση πίνακα. Αρχικά, παρουσιάζεται ένας αλγόριθμος, που χρησιμοποιείται σε περιπτώσεις κρυπτογράφησης τετραγωνικών πινάκων. Τρόποι

εφαρμογής της ίδιας μεθοδολογίας εξετάζονται προκειμένου να υλοποιηθούν σε περιπτώσεις μη τετραγωνικών πινάκων. Μία τεχνική αναδιάταξης αναλύεται, η οποία έχει ως στόχο την ποιοτική βελτίωση των αποτελεσμάτων της κρυπτογράφησης με την υλοποίηση του προτεινόμενου αλγορίθμου.

Στη συνέχεια του κεφαλαίου παρουσιάζονται ορισμένα μέτρα αξιολόγησης της κρυπτογράφησης. Τέλος παρουσιάζονται τα συμπέρασματα που εξήχθησαν με τη χρήση των παραπάνω μέτρων όσον αφορά τους αλγορίθμους και τις τεχνικές που προτείνονται.

Στο τέλος της παρούσας πτυχιακής υπάρχουν δύο παραρτήματα. Στο παράρτημα Α υπάρχουν ιστορικές αναδρομές για τον Fibonacci και τον Lester Hill. Στο παράρτημα Β παρουσιάζονται οι κώδικες που υλοποιήθηκαν στην συγκεκριμένη πτυχιακή σε προγραμματιστικό περιβάλλον MATLAB 2015, [12].

Ο αναγνώστης στη μελέτη του να λάβει υπόψη ότι κάθε κεφάλαιο αυτής της πτυχιακής εργασίας αριθμείται και υποδιαιρείται σε ενότητες, οι οποίες αριθμούνται με δυο αριθμούς, ενώ μερικές αριθμούνται με τρεις. Ο πρώτος αριθμός αναφέρεται στο κεφάλαιο, ο δεύτερος στην ενότητα και ο τρίτος, όπου υπάρχει, στην υποδιαίρεσή της. Επίσης, οι ορισμοί, τα θεωρήματα, οι προτάσεις, τα παραδείγματα, τα σχήματα και οι πίνακες αριθμούνται με δύο αριθμούς, από τους οποίους ο πρώτος αντιστοιχεί στο κεφάλαιο και ο δεύτερος στη σειρά εμφάνισής τους στο κεφάλαιο.

Κεφάλαιο 1

Βασικές Έννοιες

1.1 Βασικές Έννοιες στην ακολουθία Fibonacci

1.1.1 Ορισμός ακολουθίας

Ακολουθία πραγματικών αριθμών ονομάζουμε μια οποιοδήποτε απεικόνιση της μορφής :

$$a : \mathbb{N} \to \mathbb{R}$$

με πεδίο ορισμού το σύνολο των φυσικών αριθμών, $\mathbb{N}$, και τιμές στο σύνολο των πραγματικών αριθμών, $\mathbb{R}$. Με λίγα λόγια μια ακολουθία είναι μια άπειρη διαδοχή αριθμών και συμβολίζεται a_n. Η κάθε τιμή της ακολουθίας ονομάζεται **όρος** της ακολουθίας. Η ανεξάρτητη μεταβλητή n ονομάζεται **δείκτης** του όρου της ακολουθίας, παίρνει τιμές από το σύνολο των φυσικών αριθμών $\mathbb{N}$ και δείχνει τη σειρά της επιλογής των όρων της ακολουθίας. Δηλαδή, ο όρος a_{n-1} είναι ο προηγούμενος όρος του a_n, αντίστοιχα ο a_{n+1} είναι ο επόμενος.

Τέλος σημειώνεται με $a_n = a(n), \quad n \in \mathbb{N}$, ο **γενικός όρος** της ακολουθίας όταν αυτός δίνεται ως συνάρτηση της ανεξάρτητης μεταβλητής $n \in \mathbb{N}$.

Στην περίπτωση που η ακολουθία ορίζεται από έναν τύπο που καλεί άλλους όρους της, τότε αυτός ονομάζεται **αναδρομικός τύπος,** ο οποίος μας επιτρέπει τον υπολογισμό οποιουδήποτε όρου της αρκεί να γνωρίζουμε όλους τους προηγούμενους όρους της. Για να ξεκινήσει ο υπολογισμός απαιτείται η γνώση του πρώτου ή των πρώτων όρων της, οι οποίοι ονομάζονται **αρχικές συνθήκες**. Να σημειώσουμε ότι ο ίδιος αναδρομικός τύπος για διαφορετικές αρχικές συνθήκες παράγει διαφορετικές ακολουθίες.

Παράδειγμα 1.1

Ορισμένοι τύποι ακολουθιών δίνονται στη συνέχεια:

i. Η ακολουθία με γενικό όρο $a_n = n$ έχει όρους $1,2,3,4,5,\ldots,n,\ldots$

ii. Η ακολουθία με γενικό όρο $a_n = 2$ έχει όρους σταθερούς $2,2,2,2,2,\ldots$.

iii. Η ακολουθία με γενικό όρο $a_n = k+n$, για κάθε $k \in \mathbb{R}$, έχει όρους $k+1, k+2, k+3, \ldots, k+n, \ldots$

iv. Η ακολουθία με αναδρομικό όρο $a_{n+2} = a_{n+1} + a_n$ και αρχικούς όρους $a_1 = a_2 = 1$ έχει όρους $1,1,2,3,5,8,13,\ldots$.

1.1.2 Ορισμός γενικευμένης ακολουθίας Fibonacci

Μία από τις σπουδαιότερες ακολουθίες στα Μαθηματικά είναι η ακολουθία Fibonacci. Έχει αρκετές εφαρμογές σε πολλούς επιστημονικούς τομείς, όπως είναι η Φυσική, η Πληροφορική και η Βιολογία. Η **γενικευμένη ακολουθία Fibonacci** περιγράφεται από τον ακόλουθο αναδρομικό τύπο

$$f_n = c_1 f_{n-1} + c_2 f_{n-2} + \ldots + c_k f_{n-k} = \sum_{j=1}^{k} c_j f_{n-j} \ , \quad \text{για κάθε } n \geq k+1 \tag{1}$$

με

$$f_1 = f_2 = \ldots = f_k = 1 \tag{2}$$

όπου $c_1, c_2, \ldots, c_k$ τυχαίοι πραγματικοί αριθμοί.

Αν $c_1 > 0, c_2, c_3, \ldots, c_k \geq 0$ είναι προφανές από (1) - (2) ότι όλοι οι όροι f_n της γενικευμένης ακολουθίας Fibonacci είναι θετικοί πραγματικοί αριθμοί, που στη συνέχεια η συγκεκριμένη ακολουθία σημειώνεται $\left(f_n\left(c_1, c_2, \ldots, c_k\right)\right)_{n=1,2,\ldots}$.

Παρατήρηση 1.1

i. Από (1) – (2) διαπιστώνουμε ότι για $k=1$ ο n-οστός όρος f_n της συγκεκριμένης γενικευμένης ακολουθίας Fibonacci είναι ίσος με $f_n = c_1^{n-1}, c_1 > 0$. Θεωρήστε $k \geq 2$, διότι το $k=1$ είναι μια σπάνια περίπτωση.

ii. Έπειτα να σημειώσουμε ότι για $k \geq 2$ και $c_1 > 0, c_2 = c_3 = ... = 0$, ο n-οστός όρος f_n της γενικευμένης ακολουθίας Fibonacci $\left(f_n(c_1, 0, ..., 0)\right)_{n=1,2,...}$ είναι ίσος με $f_n = c_1^{n-k}, c_1 > 0$. Επίσης, θεωρούμε ότι υπάρχουν δύο μη μηδενικοί συντελεστές $c_i, i = 1, 2, ..., k$ στην (1), διότι διαφορετικά είναι μία ασήμαντη περίπτωση.

iii. Για $c_1 = c_2 = ... = c_k = 1$ η γενικευμένη ακολουθία Fibonacci $\left(f_n(1, 1, ..., 1)\right)_{n=1,2,...}$ για διάφορες τιμές της μεταβλητής k μας δίνει γνωστές ακολουθίες.

Συγκεκριμένα,

- Για $k = 2$, οι σχέσεις (1) – (2) παράγουν τη γνωστή ακολουθία Fibonacci 1,1,2,3,5,8,13…. , βλέπε, Παράδειγμα 1.1 (iv).
- Για $k = 3$, οι (1) – (2) μας δίνουν την ακολουθία tribonacci 1,1,1,3,5,9,17,…
- Για $k = 4$, οι (1) – (2) μας δίνουν την ακολουθία tetranacci 1,1,1,1,4,7,13,…

1.1.3 Κλασικός ορισμός ακολουθίας Fibonacci

Όπως είδαμε στην Παρατήρηση 1.1(iii) και για $k = 2$, η γνωστή ακολουθία Fibonacci 1,1,2,3,5,8,13,21… είναι μια πολύ συγκεκριμένη και ειδική υποπερίπτωση της γενικευμένης ακολουθίας Fibonacci, που ορίστηκε στην (1) - (2), αρκεί να τη σημειώσουμε ως εξής:

$$f_n = f_{n-1} + f_{n-2}, \text{ για κάθε } n \geq 3 \text{ και αρχικές συνθήκες } f_1 = 1, f_2 = 1 \qquad (3)$$

δηλαδή, για διάφορα n με $n \geq 3$ μπορούμε να βρούμε τον επόμενο όρο της ακολουθίας από τους δύο προηγούμενους του, αρκεί να χρησιμοποιήσουμε τον παραπάνω αναδρομικό τύπο, όπως παρουσιάζεται στα επόμενα παραδείγματα.

Παράδειγμα 1.2

i. Για $n = 3$, $f_3 = f_2 + f_1 = 1 + 1 = 2$

ii. Για $n = 4$, $f_4 = f_3 + f_2 = 3$

Παράδειγμα 1.3

Αν χρησιμοποιήσουμε ως αρχικές συνθήκες $f_1 = 2$, $f_2 = 1$, στον κλασικό ορισμό της ακολουθίας Fibonacci προκύπτει η ακολουθία 2, 1, 3, 4, 7, 11 , 18, 23,…

1.1.4 Σχέση Πινάκων και όρων της γενικευμένης ακολουθίας Fibonacci

Ο πίνακας της γενικευμένης ακολουθίας Fibonacci παρουσιάστηκε για πρώτη φορά στο [17] και ορίζεται ως ένας $k \times k$ μη αρνητικός πίνακας ως εξής:

$$Q_k\left(c_1, c_2, ..., c_k\right) = \begin{pmatrix} Q_1 & c_k \\ I_{k-1} & Q_2 \end{pmatrix} = \begin{pmatrix} c_1 & c_2 & c_3 & \cdots & c_k \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \tag{4}$$

όπου Q_1 είναι ένας $1 \times (k-1)$ πίνακας-γραμμή με στοιχεία τους μη αρνητικούς πραγματικούς αριθμούς $c_1 > 0, c_2, c_3, ..., c_{k-1}$, όταν $k \geq 2$. Επίσης, I_{k-1} ορίζεται ο $(k-1) \times (k-1)$ μοναδιαίος πίνακας. Τέλος ο Q_2 είναι ο $(k-1) \times 1$ πίνακας-στήλη, στον οποίο όλα του τα στοιχεία είναι ίσα με το μηδέν. Ο πίνακας $Q_k\left(c_1, c_2, ..., c_k\right)$ ονομάζεται **γενικευμένος k-Fibonacci πίνακας**.

Παρατήρηση 1.2

i. Στα [3,5,6], η ορίζουσα του γενικευμένου k-Fibonacci πίνακα είναι

$$det\left(Q_k\left(c_1, c_2, ..., c_k\right)\right) = (-1)^{k+1} c_k, \tag{5}$$

και το χαρακτηριστικό πολυώνυμο

$$x_{Q_k(c_1, c_2, ..., c_k)}(\lambda) = \lambda^k - \sum_{i=1}^{k} c_i \lambda^{k-i} = \lambda^k - c_1\lambda^{k-1} - c_2\lambda^{k-2} - \cdots - c_{k-1}\lambda - c_k \tag{6}$$

ii. Από την (5) προκύπτει ότι $Q_k(c_1,c_2,...,c_k)$ είναι ένας αντιστρέψιμος αν και μόνο αν $c_k \neq 0$ αν και μόνο αν οι ιδιοτιμές του $Q_k(c_1,c_2,...,c_k)$ είναι μη μηδενικές.

iii. Για $c_1 = c_2 = ... = c_k = 1$ η σχέση μεταξύ των αριθμών Fibonacci και των πινάκων Fibonacci $Q_k(1,1,...,1)$ και των δυνάμεων του $Q_k(1,1,...,1)$ έχουν συζητηθεί στο [3,7,8,13,15].

iv. Ο γενικευμένος 2-Fibonacci πίνακας ορίζεται στην (4) για $k=2$, $c_1 > 0, c_2 \geq 0$ είναι ο 2×2 μη αρνητικός πίνακας:

$$Q_2(c_1,c_2) = \begin{pmatrix} c_1 & c_2 \\ 1 & 0 \end{pmatrix} \tag{7}$$

Παρατήρηση 1.3

Γνωστές ακολουθίες μπορούν να αναπαρασταθούν μέσω του αντίστοιχου *k* - Fibonacci πίνακα, όπως αυτός παράγεται για τις διάφορες τιμές του *k:*

i. Για *k = 2*, η ακολουθία Fibonacci έχει αντίστοιχο πίνακα τον

$$Q_2(c_1,c_2) = \begin{pmatrix} c_1 & c_2 \\ 1 & 0 \end{pmatrix}$$

ii. Για *k* = 3 η ακολουθία Fibonacci έχει αντίστοιχο πίνακα τον

$$Q_3(c_1,c_2,c_3) = \begin{pmatrix} c_1 & c_2 & c_3 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

iii. Για *k* = 4 η ακολουθία Fibonacci έχει αντίστοιχο πίνακα τον

$$Q_4(c_1,c_2,c_3,c_4) = \begin{pmatrix} c_1 & c_2 & c_3 & c_4 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Στη συνέχεια αναφέρουμε μία πρόταση, όπου υπολογίζεται η n-στή δύναμη του γενικευμένου 2-Fibonacci πίνακα, η οποία αποδεικνύεται [1].

Θεώρημα 1.1

Έστω $c_1, c_2 > 0$ θετικοί πραγματικοί αριθμοί και ο γενικευμένος 2-Fibonacci πίνακας $Q_2(c_1, c_2)$, όπως (7). Αν $n \geq 2$, τότε η n-στή δύναμη του $Q_2(c_1, c_2)$ είναι:

$$Q_2^n(c_1, c_2) = \left(Q_2(c_1, c_2)\right)^n = \left(Q_2(c_1, c_2)\right)^{n-1} Q_2(c_1, c_2) = \begin{pmatrix} q_{11}^n & q_{12}^n \\ q_{21}^n & q_{22}^n \end{pmatrix}, \tag{8}$$

όπου οι θετικοί πραγματικοί αριθμοί $q_{11}^n, q_{12}^n, q_{21}^n, q_{22}^n$ δίνονται από τους παρακάτω τύπους:

$$q_{11}^n = \sum_{r=0}^{\left\lfloor \frac{n}{2} \right\rfloor} \binom{n-r}{r} c_1^{n-2r} c_2^r, \tag{9}$$

$$q_{12}^n = \sum_{r=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-1-r}{r} c_1^{n-1-2r} c_2^{r+1}, \tag{10}$$

$$q_{21}^n = \sum_{r=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor} \binom{n-1-r}{r} c_1^{n-1-2r} c_2^r, \tag{11}$$

$$q_{22}^n = \sum_{r=0}^{\left\lfloor \frac{n-2}{2} \right\rfloor} \binom{n-2-r}{r} c_1^{n-2-2r} c_2^{r+1}, \tag{12}$$

με $\lfloor n \rfloor$ σημειώνεται το κάτω ακέραιο μέρος του n .

Παρατήρηση 1.4

i. Αντικαθιστώντας $c_1 = c_2 = 1$ στους τύπους (9)-(12) υπολογίζονται τα στοιχεία του $Q_2^n(1,1)$ της (8) του θεωρήματος 1.1 και τελικά ο πίνακας $Q_2^n(1,1)$ είναι :

$$Q_2^n(1,1)=\begin{pmatrix} \sum_{r=0}^{\left\lfloor \frac{n}{2} \right\rfloor}\binom{n-r}{r} & \sum_{r=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor}\binom{n-1-r}{r} \\ \sum_{r=0}^{\left\lfloor \frac{n-1}{2} \right\rfloor}\binom{n-1-r}{r} & \sum_{r=0}^{\left\lfloor \frac{n-2}{2} \right\rfloor}\binom{n-2-r}{r} \end{pmatrix}. \tag{13}$$

Επίσης τα στοιχεία του πίνακα $Q_2^n(1,1)$ σχετίζονται με τους αντίστοιχους όρους της γνωστής ακολουθίας Fibonacci στην (3) και οι αντίστοιχοι τύποι έχουν αποδειχθεί [2, Θεώρημα 3.4]. Συγκεκριμένα, ο τύπος του πίνακα $Q_2^n(1,1)$ δίνεται [1, Παρατήρηση 3.1(iii)] και είναι :

$$Q_2^n(1,1)=\begin{pmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{pmatrix} \tag{14}$$

Τα στοιχεία f_{n+1}, f_n, f_{n-1} είναι οι αριθμοί Fibonacci για $n \geq 2$, οι οποίοι συνεπάγονται από την (1) - (2) για $c_1 = c_2 = 1$.

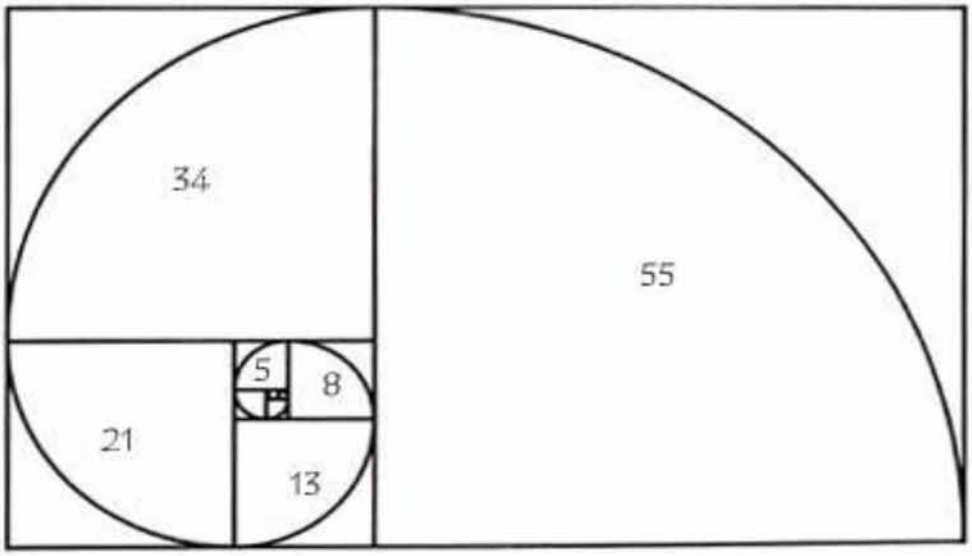
Συνδυάζοντας τους δύο τύπους (13) και (14) όλοι οι όροι της γνωστής ακολουθίας Fibonacci στην (3) μπορούν να εκφραστούν ως άθροισμα κατάλληλων διωνυμικών συντελεστών με τον εξής τρόπο:

$$f_{n+1}=\sum_{r=0}^{\left\lfloor \frac{n}{2} \right\rfloor}\binom{n-r}{r}, \text{ για } n \geq 2$$

Η γενική ιδέα της κρυπτογραφίας Fibonacci είναι βασισμένη στον πίνακα $Q_2^n(1,1)$ στη (14). Χρησιμοποιώντας τη διαδικασία της κρυπτογράφησης σε ένα μήνυμα ο γενικευμένος πίνακας 2-Fibonacci $Q_2^n(c_1,c_2)$ στην (8) για τυχαία $c_1, c_2 > 0$, προσφέρει καλύτερη ασφάλεια για κρυπτογράφηση και αποκρυπτογράφηση, επειδή $Q_2^n(c_1,c_2)$ είναι αντιστρέψιμος (Παρατήρηση 1.2(ii)) και τα στοιχεία του πίνακα $Q_2^n(c_1,c_2)$ που προκύπτουν από τους τύπους (9) - (12) μπορούν να υπολογιστούν εκ των προτέρων για τις διάφορες τιμές των c_1, c_2.

1.1.5 Η «Χρυσή Σπείρα»

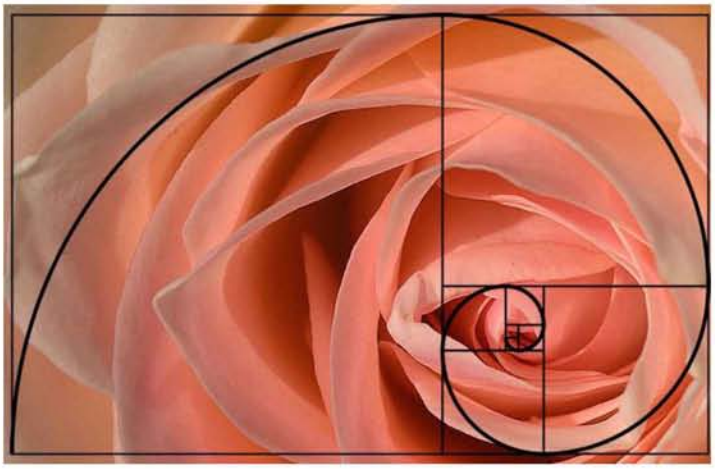
Η 2-Fibonacci (Παρατήρηση 1.1(iii)) ακολουθία είναι αρκετά σημαντική λόγω της γεωμετρικής της ερμηνείας και κάποιων μαθηματικών σχέσεων που προκύπτουν από αυτή, όπως παρουσιάζεται στα ακόλουθα σχήματα.



Σχήμα 1.1: Χρυσή Σπείρα

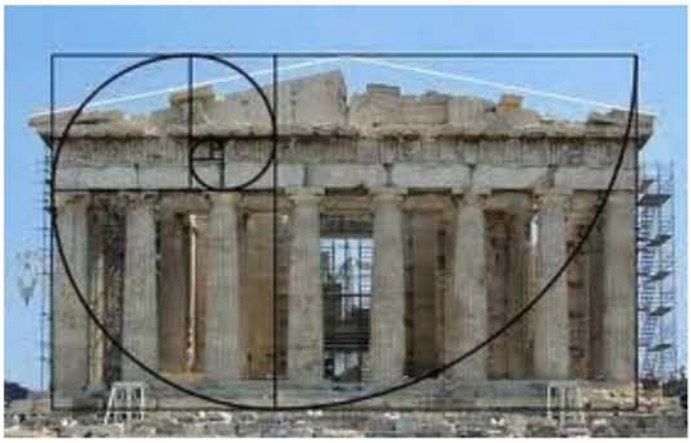
Παρατηρούμε ότι στο Σχήμα 1.1 το εμβαδόν του κάθε τετραγώνου αντιστοιχεί σε έναν αριθμό Fibonacci. Επίσης το εμβαδόν του σχήματος είναι ίσο με το συνολικό άθροισμα των τιμών των τετραγώνων $E = 1^2 + 1^2 + 2^2 + 3^2 + 5^2 + 8^2 + 13^2 + 21^2 + 34^2 = 1870$ (34 x 55).

Η χρυσή σπείρα είναι ένα αξιοσημείωτο μαθηματικό φαινόμενο, το οποίο το συναντάμε συνέχεια στην καθημερινότητα μας (Σχήμα 1.2) αλλά και στο γαλαξιακό μας σύστημα (Σχήμα 1.3) και σε σπουδαία αρχιτεκτονικά κτίρια της αρχαιότητας (Σχήμα 1.4).



Σχήμα 1.2

Σχήμα 1.3



Σχήμα 1.4

1.1.6 Άλλες γνωστές αναδρομικές ακολουθίες

Όπως είδαμε στο υποκεφάλαιο 1.1.2 η ακολουθία Fibonacci έχει αρχικές συνθήκες $f_1 = 1, f_2 = 1$ και τύπο $f_n = f_{n-1} + f_{n-2}$. Εκτός όμως από τη συγκεκριμένη ακολουθία υπάρχουν και άλλες ακολουθίες, που έχουν παρόμοιες ιδιότητες με τη διαφορά ότι έχουν διαφορετικές αρχικές συνθήκες. Κάποιες από αυτές είναι οι εξής:

- **Padovan** $a_n = a_{n-2} + a_{n-3}$ με αρχικές συνθήκες $a_1 = 1, a_2 = a_3 = 0$
- **Lucas** $l_n = l_{n-1} + l_{n-2}$ με αρχικές συνθήκες $l_1 = 2, l_2 = 1$

Επίσης υπάρχουν και οι ακολουθίες που έχουν διαφορετικό αναδρομικό τύπο, για παράδειγμα

- **Tribonacci** $f_n = f_{n-1} + f_{n-2} + f_{n-3}$, με αρχικές συνθήκες $f_1 = f_2 = 1, f_3 = 2$
- **Tetranacci** $f_n = f_{n-1} + f_{n-2} + f_{n-3} + f_{n-4}$, με αρχικές συνθήκες $f_1 = f_2 = 1, f_3 = 2, f_4 = 4$

Στη συγκεκριμένη πτυχιακή θα ασχοληθούμε με τις γενικευμένες ακολουθίες Fibonacci που περιγράψαμε στην Παράγραφο 1.1.2. τους πίνακες που παράγονται από τις συγκεκριμένες ακολουθίες και τις εφαρμογές που μπορεί να έχουν στην Κρυπτογραφία.

1.1.7 Ορισμένοι ορισμοί από Γραμμική Άλγεβρα

Ορισμός 1.1 [4]

Έστω $A \in R^{m \times n}$ και $B \in R^{p \times q}$. Τότε το **γινόμενο Kronecker** των A και B είναι ο εξής πίνακας:

$$A \otimes B = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{m1}B & \cdots & a_{mn}B \end{pmatrix} \in R^{mp \times nq}$$

Είναι προφανές ότι $A \otimes B \neq B \otimes A$.

Παράδειγμα 1.4

Έστω $A=\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}$ και $B=\begin{pmatrix}0 & 5\\ 6 & 7\end{pmatrix}$ το αποτέλεσμα της πράξης του Kronecker βγαίνει ως εξής :

$$\begin{pmatrix}1 & 2\\ 3 & 4\end{pmatrix}\otimes\begin{pmatrix}0 & 5\\ 6 & 7\end{pmatrix}=\begin{pmatrix}1\cdot\begin{pmatrix}0 & 5\\ 6 & 7\end{pmatrix} & 2\cdot\begin{pmatrix}0 & 5\\ 6 & 7\end{pmatrix}\\ 3\cdot\begin{pmatrix}0 & 5\\ 6 & 7\end{pmatrix} & 4\cdot\begin{pmatrix}0 & 5\\ 6 & 7\end{pmatrix}\end{pmatrix}=\begin{pmatrix}1\cdot 0 & 1\cdot 5 & 2\cdot 0 & 2\cdot 5\\ 1\cdot 6 & 1\cdot 7 & 2\cdot 6 & 2\cdot 7\\ 3\cdot 0 & 3\cdot 5 & 4\cdot 0 & 4\cdot 5\\ 3\cdot 6 & 3\cdot 7 & 4\cdot 6 & 4\cdot 7\end{pmatrix}=\begin{pmatrix}0 & 5 & 0 & 10\\ 6 & 7 & 12 & 14\\ 0 & 15 & 0 & 20\\ 18 & 21 & 24 & 28\end{pmatrix}$$

1.2 Βασικές έννοιες σχετικά με την Κρυπτογραφία

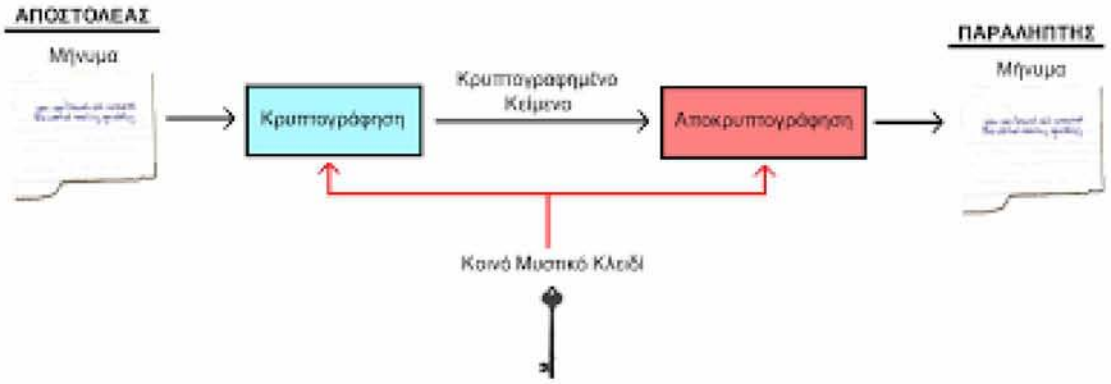
Στις μέρες μας η τεχνολογία αναπτύσσεται με φρενήρη ρυθμό, συνεχώς παρουσιάζονται νέες τεχνολογίες που ζητούν τα προσωπικά μας δεδομένα. Αυτό έχει ως αποτέλεσμα τα προσωπικά μας δεδομένα και η προσωπική μας ζωή, με την πάροδο του χρόνου να εξαλείφονται και να χάνουν την πραγματική τους έννοια. Για το λόγο αυτό αναπτύχθηκε ο κλάδος της Κρυπτογραφίας, βασιζόμενος στην Ασφάλεια Συστημάτων, ώστε να δημιουργηθούν τρόποι αντιμετώπισης του συγκεκριμένου προβλήματος, το οποίο με τον καιρό παίρνει πολύ μεγάλες διαστάσεις. Παρακάτω αναλύονται κάποιοι βασικοί όροι της Κρυπτογραφίας [10].

1.2.1 Βασικοί Ορισμοί

- **Κρυπτογράφηση**: Διαδικασία με την οποία μετατρέπουμε τα δεδομένα σε μη αναγνώσιμη μορφή
- **Αποκρυπτογράφηση:** Αντίστροφη διαδικασία της κρυπτογράφησης, δηλαδή, η μετατροπή των κρυπτογραφημένων σε αναγνώσιμη μορφή
- **Κλειδί**: Μία συμβολοακολουθία η οποία χρησιμοποιείται είτε για κρυπτογράφηση είτε για αποκρυπτογράφηση. Χωρίζονται σε δημόσια και ιδιωτικά
- **Αρχικό Κείμενο (Plaintext)**: Είναι το μήνυμα που θα υποστεί τη διαδικασία της κρυπτογράφησης.
- **Κρυπτογραφημένο Κείμενο (Ciphertext)**: Είναι το αποτέλεσμα της διαδικασίας της κρυπτογράφησης.

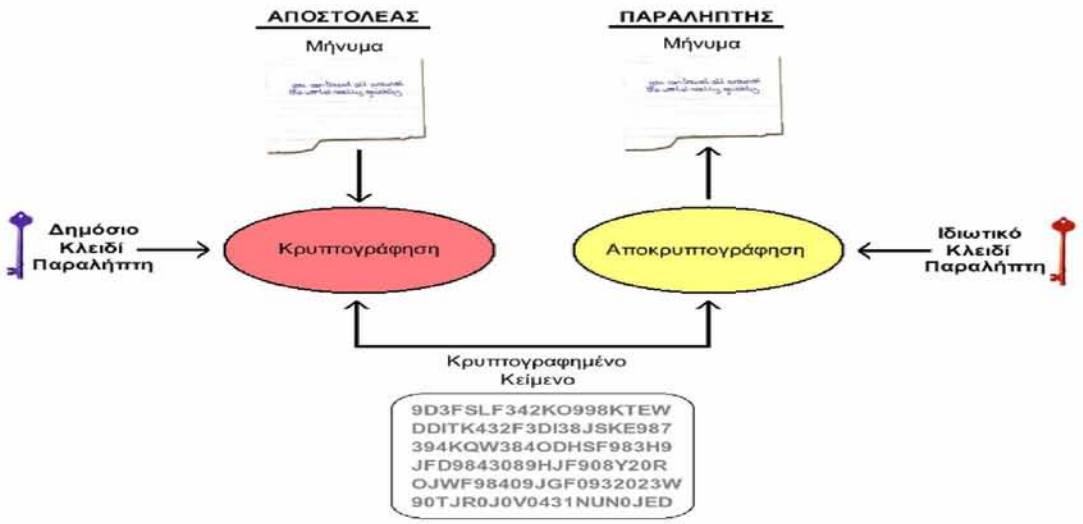
1.2.2 Είδη Κρυπτογράφησης

Η Κρυπτογράφηση χωρίζεται σε δύο μεγάλες κατηγορίες, στη **συμμετρική** και στη **μη συμμετρική**.



Σχήμα 1.5

Στο Σχήμα 1.5 παρουσιάζεται η λειτουργία της συμμετρικής κρυπτογράφησης. Παρατήρουμε ότι χρησιμοποιείται **ένα μοναδικό** κλειδί για τη διαδικασία της κρυπτογράφησης και της αποκρυπτογράφησης, το οποίο είναι ιδιωτικό. Το συγκεκριμενό κλειδί το γνωρίζουν μόνο ο αποστολέας και ο παραλήπτης για αυτό ονομάζεται **ιδιωτικό**. Όταν διαρρεύσει το κλειδί, τότε η διαδικασία της κρυπτογράφησης είναι αποτυχημένη. Το συγκεκριμένο είδος κρυπτογράφησης για να λειτουργήσει σωστά, πρέπει να υπάρχει ένα ασφαλές κανάλι, ώστε να μπορέσει ο αποστολέας και ο παραλήπτης να ανταλλάξουν το ιδιωτικό τους κλειδί. Γνωστοί συμμετρικοί αλγόριθμοι είναι DES, RC5, DESX.



Σχήμα 1.6

Στο Σχήμα 1.6 βλέπουμε πως λειτουργούν οι μη συμμετρικοί αλγόριθμοι κρυπτογράφησης. Σε αντίθεση με την προηγούμενη κατηγορία, εδώ, χρειάζονται **δύο** κλειδιά, **ένα δημόσιο**, το οποίο το χρησιμοποιεί ο αποστολέας για να πραγματοποιήσει τη διαδικασία της κρυπτογράφησης και είναι γνωστό σε όλους και **ένα ιδιωτικό**, το οποίο γνωρίζει μόνο ο παραλήπτης και το χρησιμοποιεί για να αποκρυπτογραφήσει το κρυπτογραφημένο κείμενο (Ciphertext). Στο συγκεκριμένο είδος κρυπτογράφησης δεν χρειάζεται να υπάρχει ένα ασφαλές κανάλι ανάμεσα στον αποστολέα και στον παραλήπτη, όπως στη συμμετρική κρυπτογράφηση. Κάποιοι ασσύμετροι αλγόριθμοι είναι οι RSA, DSA.

1.2.3 Αλγόριθμος του Hill

Στην παρούσα πτυχιακή εργασία χρησιμοποιείται το πρώτο είδος κρυπταλγορίθμων (συμμετρικοί) και συγκεκριμένα ο **αλγόριθμος του Hill** [21, 22]. Ο γενικός τύπος της κρυπτογράφησης στον αλγόριθμο του Hill είναι ο εξής:

$$C = (KP) \bmod n \tag{15}$$

όπου C είναι το κρυπτογραφημένο κείμενο, K είναι ένας $k \times k$ αντιστρέψιμος πίνακας, ο οποίος είναι το κρυφό κλειδί, P το αρχικό κείμενο και n είναι ένας

ακέραιος αριθμός, ο οποίος είναι η μέγιστη πιθανή τιμή μέσα από το σύνολο τιμών που περιέχει το P.

Ο τύπος της αποκρυπτογράφησης είναι ο εξής:

$$P = (K^{-1}C) \bmod n \tag{16}$$

όπου K^{-1} συμβολίζει τον αντίστροφο πίνακα του K με K, C, n δίνονται στη (15).

Απαραίτητες προϋποθέσεις για να λειτουργήσει ο αλγόριθμος του Hill είναι :

i) $\det K \neq 0$, για να αντιστρέφεται ο πίνακας K,

ii) $\gcd(\det K, n) = 1$, όπου $\gcd(\det K, n)$ ο μέγιστος κοινός διαιρέτης της ορίζουσας του K και του n, δηλαδή, οι δύο τιμές να είναι πρώτοι αριθμοί μεταξύ τους.

Επιπλέον, ο αντίστροφος πίνακας δίνεται από

$$K^{-1} = \left((\det K)^{-1} adjK\right) \bmod n \tag{17}$$

όπου $adjK$ συμβολίζει τον προσαρτημένο πίνακα του K και δίνεται από τον τύπο

$$adjK = \begin{pmatrix} \det K_{11} & -\det K_{21} & \dots & (-1)^{k+1} \det K_{k1} \\ \vdots & \vdots & \ddots & \vdots \\ (-1)^{k+1} \det K_{1k} & (-1)^{k+2} \det K_{2k} & \dots & (-1)^{2k} \det K_{kk} \end{pmatrix} \tag{18}$$

και K_{ij} είναι ο $(k-1)\times(k-1)$ υποπίνακας του K χωρίς την i-γραμμή και j-στήλη.

Παράδειγμα 1.4

Έστω ότι το κλειδί είναι ο πίνακας $K = \begin{pmatrix} 3 & 2 \\ 8 & 9 \end{pmatrix}$

Ο αποστολέας κρυπτογραφεί το μήνυμα « ΓΕΙΑ » με τον αλγόριθμο του Hill. Το n στην περίπτωση αυτή είναι 24, διότι χρησιμοποιείται το ελληνικό αλφάβητο που αποτελείται από 24 γράμματα, άρα το P λαμβάνει τις τιμές στο διάστημα 0 εώς 23. Αρχικά ελέγχουμε αν ικανοποιούνται οι παραπάνω συνθήκες (i) και (ii).

Επειδή $\det K = 11$, K είναι αντιστρέψιμος και $\gcd(11, 24) = 1$, άρα μπορεί ο K να είναι κλειδί.

Στη συνέχεια χωρίζεται το μήνυμα σε πίνακες, που οι γραμμές του είναι ίσες με τις στήλες του πίνακα K για να μπορέσει να υλοποιήθει η πράξη του πολλαπλασιασμού των πινάκων και να γίνει η κρυπτογράφηση (βλ. Υποενότητα 1.2.3).

Το κάθε γράμμα του ελληνικού αλφαβήτου αντιστοιχεί σε έναν αριθμό.

Α = 0, Β = 1 , Γ = 2 ... Ω = 23

Άρα το μήνυμα χωρίζεται σε 2 πίνακες $\Gamma\Epsilon = \begin{pmatrix} 2 \\ 4 \end{pmatrix}, \text{IA} = \begin{pmatrix} 8 \\ 0 \end{pmatrix}$

Χρησιμοποιώντας τον τύπο (15) της κρυπτογράφησης έχουμε

$$C_1 = \left[\begin{pmatrix} 3 & 2 \\ 8 & 9 \end{pmatrix} \begin{pmatrix} 2 \\ 4 \end{pmatrix} \right] \bmod 24 = \begin{pmatrix} 14 \\ 52 \end{pmatrix} \bmod 24 = \begin{pmatrix} 14 \\ 4 \end{pmatrix}$$

Άρα το ΓΕ μετά την κρυπτογράφηση γίνεται ΟΕ

Αντίστοιχα $C_2 = \left[\begin{pmatrix} 3 & 2 \\ 8 & 9 \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix} \right] \bmod 24 = \begin{pmatrix} 24 \\ 16 \end{pmatrix} \bmod 24 = \begin{pmatrix} 0 \\ 16 \end{pmatrix}$ Άρα ΑΡ

Τελικά η λέξη «ΓΕΙΑ» μετατρέπεται σε «ΟΕΑΡ»

Τώρα πρέπει ο παραλήπτης να αποκρυπτογραφήσει το συγκεκριμένο κείμενο χρησιμοποιώντας το κλειδί K κάνοντας την αντίστροφη διαδικασία. Αρχικά από τη (17) υπολογίζεται ο αντίστροφος πίνακας του K, που είναι :

$$K^{-1} = \left[11^{-1} \begin{pmatrix} 9 & -2 \\ -8 & 3 \end{pmatrix} \right] \bmod 24$$

Με τον αλγόριθμο του Ευκλείδη [13] υπολογίζεται το $11^{-1} \bmod 24$ ως εξής:

$$24 = 2 \cdot 11 + 2$$

$$11 = 5 \cdot 2 + 1$$

$$2 = 2 \cdot 1 + 0$$

Άρα

$$1 = 11 - 5 \cdot 2 = 11 - 5 \cdot (24 - 2 \cdot 11) = -5 \cdot 24 + 11 \cdot 11$$

Άρα $11^{-1} \bmod 24 = 11 \bmod 24 = 11$, οπότε ο αντίστροφος είναι

$$K^{-1}=\left[11\cdot\begin{pmatrix}9 & -2\\ -8 & 3\end{pmatrix}\right]\bmod 24=\begin{pmatrix}99 & -22\\ -88 & 33\end{pmatrix}\bmod 24=\begin{pmatrix}3 & 2\\ 8 & 9\end{pmatrix}$$

Τέλος από τον πίνακα K^{-1} και την (16) τα ζεύγη του αποκρυπτογραφημένου είναι

$$P_1=\left[\begin{pmatrix}3 & 2\\ 8 & 9\end{pmatrix}\begin{pmatrix}14\\ 4\end{pmatrix}\right]\bmod 24=\begin{pmatrix}2\\ 4\end{pmatrix}$$

$$P_2=\left[\begin{pmatrix}3 & 2\\ 8 & 9\end{pmatrix}\begin{pmatrix}0\\ 16\end{pmatrix}\right]\bmod 24=\begin{pmatrix}8\\ 0\end{pmatrix}$$

Άρα $P_1 \| P_2 = \text{ΓΕΙΑ}$ το οποίο είναι το αρχικό κείμενο που έστειλε ο αποστολέας.

Κεφάλαιο 2

Υλοποίηση Κρυπταλγορίθμων

Στο συγκεκριμένο κεφάλαιο παρουσιάζεται ο σχεδιασμός και η υλοποίηση του αλγόριθμου που δημιουργήθηκε. Στο συγκεκριμένο αλγόριθμο κρυπτογραφείται ένας τετραγωνικός πίνακας με τη χρήση των **Γενικευμένων Ακολουθιών Fibonacci** (βλ. 1.1.2) και του **αλγορίθμου του Hill** (βλ. 1.2.3)(Κώδικας Β1) και στη συνέχεια ακολουθεί η αποκρυπτογράφηση ώστε να καταλήξουμε στον αρχικό μας πίνακα (Κώδικας Β2). Οι αλγόριθμοι που δημιουργήθηκαν χρησιμοποιοιούν συμμετρικό κλειδί και οι δύο (βλ. 1.2.2). Οπότε απαιτείται η ύπαρξη ασφαλούς καναλιού επικοινωνίας για να γίνει η ανταλλαγή του συμμετρικού κλειδιού.

2.1 Αλγόριθμος Κρυπτογράφησης χωρίς αναδιάταξη

2.1.1 Υλοποίηση Αλγορίθμου Κρυπτογράφησης τετραγωνικού πίνακα χωρίς βάρη

Ο αλγόριθμος της Κρυπτογράφησης (Κώδικας Β1) παίρνει ως είσοδο τρεις μεταβλητές έναν τετραγωνικό πίνακα ($I1$), έναν θετικό ακέραιο αριθμό ($k \geq 2$), ο οποίος δηλώνει το μέγεθος του γενικευμένου k-Fibonacci πίνακα $Q_k(c_1,c_2,...,c_k)$ (βλ. Παρατήρηση 1.2) και έναν άλλο θετικό ακέραιο (t), ο οποίος δηλώνει τη δύναμη στην οποία υψώνουμε τον γενικευμένο πίνακα k-Fibonacci (Θεώρημα 1.1). Σημειώνεται ότι ο περιορισμός για τη δύναμη (t) που υψώνεται ο πίνακας $Q_k(c_1,c_2,...,c_k)$ είναι $\boldsymbol{t \geq k}$, [2, Θεώρημα 3.4].

Αρχικά καλείται η συνάρτηση size() του MATLAB 2015, η οποία υπολογίζει το μέγεθος του πίνακα $I1$, έστω m,n.

Στη συνέχεια δημιουργείται ένας πίνακας (barh) με μέγεθος $1\times(k-1)$, του οποίου όλες οι τιμές του είναι ίσες με τη μονάδα. Ελέγχει αν το πλήθος των γραμμών ή των στηλών είναι μεγαλύτερο. Αν οι στήλες είναι περισσότερες αποθηκεύει σε μια καινούρια μεταβλητή (r) το αποτέλεσμα της διαίρεσης (γραμμές / k) αλλιώς αποθηκεύει στη μεταβλητή (r) το αποτέλεσμα της διαίρεσης (στήλες / k).

Έπειτα δημιουργείται ο γενικευμένος πίνακας k-Fibonacci $Q_k\left(c_1,c_2,...,c_k\right)$, (βλ. Υποενότητα 1.1.4) ο οποίος έχει διάσταση (k x k). Στην πρώτη σειρά έχει τον πίνακα barh που δημιουργήθηκε παραπάνω, στην τελευταία στήλη στις θέσεις $(k-1)\times 1$ υπάρχουν μηδενικά και στις υπόλοιπες θέσεις υπάρχει ένας πίνακας $(k-1)\times(k-1)$.

Δημιουργεί έναν $r\times r$ μοναδιαίο πίνακα, Y. Με τη χρήση της συνάρτησης kron, η οποία υπολογίζει το γινόμενο Kronecker (Ορισμός 1.1, στην Υποενότητα 1.1.7) δημιουργείται ένας καινούριος πίνακας $Q := Y \otimes Q_k\left(c_1,c_2,...,c_k\right)$, ο οποίος υψώνεται στη δύναμη t, και δηλώνεται ως $M := Q^t$.

Στη συνέχεια βάση του αλγορίθμου Hill (βλ. Υποενότητα 1.2.3) γίνεται η πράξη της κρυπτογράφησης. Πολλαπλασιάζεται ο αρχικός πίνακας $I1$ με τον πίνακα M και προκύπτει ο $m\times n$ πίνακας A. Υπάρχει άλλος ένας πίνακας B ο οποίος έχει τις ίδιες διαστάσεις με τον A και περιέχει την πιθανή μέγιστη τιμή που μπορεί να έχει ο αρχικός πίνακας I1. Τέλος ο κρυπτογραφημένος πίνακας C είναι αποτέλεσμα της πράξης $A \bmod B$.

Παράδειγμα 2.1

Έστω ο 8×8 πίνακας $I1=\begin{pmatrix} 20 & 23 & 11 & 17 & 7 & 11 & 18 & 24 \\ 22 & 24 & 22 & 19 & 2 & 10 & 19 & 9 \\ 4 & 4 & 20 & 18 & 3 & 19 & 7 & 15 \\ 22 & 24 & 24 & 10 & 20 & 20 & 17 & 6 \\ 16 & 23 & 16 & 16 & 17 & 5 & 16 & 19 \\ 3 & 12 & 1 & 5 & 8 & 12 & 4 & 7 \\ 7 & 20 & 21 & 17 & 23 & 11 & 3 & 13 \\ 14 & 4 & 23 & 1 & 1 & 16 & 12 & 17 \end{pmatrix}$, $t=4$ και $k=4$

Ο πίνακας που δημιουργείται για τα βάρη $c_1 = c_2 = c_3 = c_4 = 1$ είναι ο 4×4 πίνακας

$$Q_4(1,1,1,1) := Q_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Παρατηρούμε ότι $c_k \neq 0$ (βλέπε, Υποενότητα 1.1.4). Στη συνέχεια θεωρούμε τον 2×2 πίνακα $Y = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, οπότε μετά από τον Kronecker προκύπτει ο 8×8 πίνακας

$$Q = Y \otimes Q_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

με $\det Q = 1$.

οπότε μετά από τον Kronecker προκύπτει ο 8×8 πίνακας

Υψώνεται ο πίνακας Q στην $t = 4$ και προκύπτει ο 8×8 πίνακας $M = Q^4$, ο οποίος είναι το κλείδι μας

$$M = Q^4 = \begin{pmatrix} 8 & 7 & 6 & 4 & 0 & 0 & 0 & 0 \\ 4 & 4 & 3 & 2 & 0 & 0 & 0 & 0 \\ 2 & 2 & 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 8 & 7 & 6 & 4 \\ 0 & 0 & 0 & 0 & 4 & 4 & 3 & 2 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Επίσης πολλαπλασιάζεται το κλειδί (M) με τον αρχικό πίνακα ($I1$) και προκύπτει ο 8×8 πίνακας A.

$$A = M \cdot I1 = \begin{pmatrix} 426 & 472 & 458 & 417 & 168 & 352 & 387 & 369 \\ 224 & 248 & 240 & 218 & 85 & 181 & 203 & 189 \\ 114 & 126 & 130 & 118 & 44 & 100 & 105 & 102 \\ 68 & 75 & 77 & 64 & 32 & 60 & 61 & 54 \\ 247 & 404 & 353 & 269 & 334 & 254 & 222 & 347 \\ 125 & 208 & 177 & 137 & 171 & 133 & 113 & 177 \\ 66 & 114 & 99 & 77 & 97 & 72 & 58 & 95 \\ 40 & 59 & 61 & 39 & 49 & 44 & 35 & 56 \end{pmatrix}$$

Έπειτα δημιουργείται ο 8×8 πίνακας

$$B = \begin{pmatrix} 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \end{pmatrix}$$

Τέλος προκύπτει ο 8×8 κρυπτογραφημένος πίνακας $C = A \bmod B$

$$C = \begin{pmatrix} 170 & 216 & 202 & 161 & 168 & 96 & 131 & 113 \\ 224 & 248 & 240 & 218 & 85 & 181 & 203 & 189 \\ 114 & 126 & 130 & 118 & 44 & 100 & 105 & 102 \\ 68 & 75 & 77 & 64 & 32 & 60 & 61 & 54 \\ 247 & 148 & 97 & 13 & 78 & 254 & 222 & 91 \\ 125 & 208 & 177 & 137 & 171 & 133 & 113 & 177 \\ 66 & 114 & 99 & 77 & 97 & 72 & 58 & 95 \\ 40 & 59 & 61 & 39 & 49 & 44 & 35 & 56 \end{pmatrix}$$

Παραπάνω αναλύθηκε βήμα-βήμα ο αλγόριθμος κρυπτογράφησης ενός τετραγωνικού πίνακα (βλέπε, Κώδικα B1), στη συνέχεια αναλύεται ο τρόπος αποκρυπτογράφησής του.

2.1.2 Υλοποίηση Αλγορίθμου Αποκρυπτογράφησης τετραγωνικού πίνακα χωρίς βάρη

Για να αποκρυπτογραφηθεί ο πίνακας C χρειάζεται μόνο ο πίνακας M με βάση τον αλγόριθμο του Hill.

Εξετάζεται εάν ο μέγιστος κοινός διαρέτης της ορίζουσας του κλειδιού ($\det M$) και του 256 είναι μονάδα, εάν ισχύει συνεχίζει, διαφορετικά αλλιώς τερματίζεται το πρόγραμμα. Δημιουργείται ένας καινούριος πίνακας R (βλ. 1.2.3) ο οποίος προκύπτει από την εξής πράξη:

$$R = \frac{1}{\det M}\left(adjM\right)\mathrm{C}$$

Τέλος $R \bmod B$ δίνει τον αρχικό πίνακα $I1$

Σχόλιο 2.1

Όταν ο αλγόριθμος αποκρυπτογράφησης δέχεται σαν είσοδο ένα πολύ μεγάλο κλειδί (M) με μεγάλες δυνάμεις (t) και μεγάλα βάρη ($c_1, c_2, \ldots, c_{k-1}$) από την εξίσωση (17), η ορίζουσα του κλειδιού ($\det M$) τείνει στο άπειρο και επειδή ο τύπος αποκρυπτογράφησης του Hill χρειάζεται τον $\det M^{-1}$ το Matlab 2015 μηδενίζει το αποτέλεσμα και δίνει σαν έξοδο έναν πίνακα, στον οποίο όλες οι τιμές είναι μηδέν.

Παράδειγμα 2.2

Χρησιμοποιώντας το κλειδί-πίνακα M και τον κρυπτογραφημένο πίνακα C από το παράδειγμα 2.1.2 η αποκρυπτογράφηση γίνεται ως εξής:

$\det M = 1$, άρα ο μέγιστος κοινός διαίρετης του της ορίζουσας και του 256 είναι η μονάδα.

Ο προσαρτημένος πίνακας

$$adjM = \begin{pmatrix} 1.0000 & -1.0000 & -1.0000 & -1.0000 & 0 & 0 & 0 & 0 \\ -1.0000 & 2.0000 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1.0000 & 2.0000 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1.0000 & 2.0000 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1.0000 & -1.0000 & -1.0000 & -1.0000 \\ 0 & 0 & 0 & 0 & -1.0000 & 2.0000 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1.0000 & 2.0000 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1.0000 & 2.0000 \end{pmatrix}$$

Άρα

$$R = \frac{1}{detM}(adjM)C = \begin{pmatrix} -236 & -233 & -245 & -239 & 7 & -245 & -238 & -232 \\ 278 & 280 & 278 & 275 & 2 & 266 & 275 & 265 \\ 4 & 4 & 20 & 18 & 3 & 19 & 7 & 15 \\ 22 & 24 & 24 & 10 & 20 & 20 & 17 & 6 \\ 16 & -233 & -240 & -240 & -239 & 5 & 16 & -237 \\ 3 & 268 & 257 & 261 & 264 & 12 & 4 & 263 \\ 7 & 20 & 21 & 17 & 23 & 11 & 3 & 13 \\ 14 & 4 & 23 & 1 & 1 & 16 & 12 & 17 \end{pmatrix}$$

Η τελική πράξη της αποκρυπτογράφησης $R \bmod B$ δίνει τον αρχικό πίνακα $I1$,

$$E = I1 = \begin{pmatrix} 20 & 23 & 11 & 17 & 7 & 11 & 18 & 24 \\ 22 & 24 & 22 & 19 & 2 & 10 & 19 & 9 \\ 4 & 4 & 20 & 18 & 3 & 19 & 7 & 15 \\ 22 & 24 & 24 & 10 & 20 & 20 & 17 & 6 \\ 16 & 23 & 16 & 16 & 17 & 5 & 16 & 19 \\ 3 & 12 & 1 & 5 & 8 & 12 & 4 & 7 \\ 7 & 20 & 21 & 17 & 23 & 11 & 3 & 13 \\ 14 & 4 & 23 & 1 & 1 & 16 & 12 & 17 \end{pmatrix}$$

2.1.3 Υλοποίηση Αλγορίθμου Κρυπτογράφησης Μη Τεραγωνικού Πίνακα με Βάρη (1η περίπτωση)

Σε αυτήν την περίπτωση χρησιμοποιούνται κάποια κοινά με τον προηγούμενο αλγόριθμο (βλέπε, Υποενότητα 2.1.2) μέχρι και τον υπολογισμό του πίνακα $M = Q^t$

ο αλγόριθμος είναι ίδιος. Επειδή θα προστεθούν βάρη, αλλάζει ο πίνακας barh. Επίσης σε αυτήν την περίπτωση πρέπει η μία διάσταση του πίνακα, που πρέπει να κρυπτογραφηθεί, να είναι πολλαπλάσια της άλλης, αυτό σημαίνει ότι $\gcd(m,n)\neq 1$ και συγκεκριμένα $\gcd(m,n)\geq 2$.

Αρχικά ο αλγόριθμος ελέγχει ποια από τις διαστάσεις m,n είναι μεγαλύτερη και αν υπάρχει κοινός διαιρέτης μεταξύ αυτών των διαστάσεων, ο οποίος να είναι μεγαλύτερος ή ίσος του 2. Κατόπιν με τη μικρότερη διάσταση που υπολογίστηκε κατά τον προηγούμενο έλεγχο, χωρίζεται ο ορθογώνιος πίνακας σε τετραγωνικούς υποπίνακες J.

Στη συνέχεια κρυπτογραφείται ο κάθε πίνακας ξεχωριστά όπως και στην προηγούμενη υποενότητα αφού οι υποπίνακες είναι τετραγωνικοί και στη συνέχεια ενώνονται σε έναν πίνακα C, ο οποίος είναι ο κρυπτογραφημένος πίνακας.

Παράδειγμα 2.3

Έστω ο παρακάτω 16×8 πίνακας, $t=4$ και $k=4$

$$I1=\begin{pmatrix}
20 & 11 & 7 & 18 & 22 & 9 & 14 & 6\\
22 & 22 & 2 & 19 & 24 & 20 & 12 & 22\\
4 & 20 & 3 & 7 & 14 & 15 & 1 & 4\\
22 & 24 & 20 & 17 & 4 & 14 & 9 & 20\\
16 & 16 & 17 & 16 & 4 & 23 & 4 & 13\\
3 & 1 & 8 & 4 & 7 & 7 & 20 & 24\\
7 & 21 & 23 & 3 & 21 & 19 & 8 & 2\\
14 & 23 & 1 & 12 & 7 & 19 & 13 & 11\\
23 & 17 & 11 & 24 & 20 & 10 & 4 & 3\\
24 & 19 & 10 & 9 & 6 & 14 & 15 & 24\\
4 & 18 & 19 & 15 & 23 & 2 & 7 & 1\\
24 & 10 & 20 & 6 & 9 & 2 & 16 & 19\\
23 & 16 & 5 & 19 & 5 & 13 & 17 & 20\\
12 & 5 & 12 & 7 & 7 & 19 & 18 & 21\\
20 & 17 & 11 & 13 & 15 & 23 & 11 & 3\\
4 & 1 & 16 & 17 & 12 & 4 & 3 & 10
\end{pmatrix}$$

Ο τυχαίος πίνακας $barh = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$ τον χρησιμοποιεί για να δημιουργήσει όπως και προηγουμένως τον 4×4 γενικευμένο Fibonacci πίνακα

$$Q_4(1,3,2,1) = \begin{pmatrix} 1 & 3 & 2 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Άρα $$Q = Y \otimes Q_4(1,3,2,1) = \begin{pmatrix} 1 & 3 & 2 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Υψώνεται ο πίνακας Q στην $t = 4$ και προκύπτει ο 8×8 πίνακας $M = Q^4$, ο οποίος είναι το κλειδί μας, που ισούται με:

$$M = Q^4 = \begin{pmatrix} 24 & 36 & 22 & 9 & 0 & 0 & 0 & 0 \\ 9 & 15 & 9 & 4 & 0 & 0 & 0 & 0 \\ 4 & 5 & 3 & 1 & 0 & 0 & 0 & 0 \\ 1 & 3 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 24 & 36 & 22 & 9 \\ 0 & 0 & 0 & 0 & 9 & 15 & 9 & 4 \\ 0 & 0 & 0 & 0 & 4 & 5 & 3 & 1 \\ 0 & 0 & 0 & 0 & 1 & 3 & 2 & 1 \end{pmatrix}$$

Στη συνέχεια υπολογίζει πόσους υποπίνακες χρειάζεται

$$\text{number of Chunks} = n / m$$

και δημιουργεί και έναν B, η διαφορά όμως είναι ότι τώρα πολλαπλασιάζεται με μικρότερους πίνακες, οπότε οι διάστασεις του είναι *mxm*.

$$B = \begin{pmatrix} 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \end{pmatrix}$$

Στο συγκεκριμένο παράδειγμα είναι προφανές οτι μπορεί να χωριστεί σε δυο πίνακες

$$J_1 = \begin{pmatrix} 20 & 11 & 7 & 18 & 22 & 9 & 14 & 6 \\ 22 & 22 & 2 & 19 & 24 & 20 & 12 & 22 \\ 4 & 20 & 3 & 7 & 14 & 15 & 1 & 4 \\ 22 & 24 & 20 & 17 & 4 & 14 & 9 & 20 \\ 16 & 16 & 17 & 16 & 4 & 23 & 4 & 13 \\ 3 & 1 & 8 & 4 & 7 & 7 & 20 & 24 \\ 7 & 21 & 23 & 3 & 21 & 19 & 8 & 2 \\ 14 & 23 & 1 & 12 & 7 & 19 & 13 & 11 \end{pmatrix}$$

ή

$$J_2 = \begin{pmatrix} 23 & 17 & 11 & 24 & 20 & 10 & 4 & 3 \\ 24 & 19 & 10 & 9 & 6 & 14 & 15 & 24 \\ 4 & 18 & 19 & 15 & 23 & 2 & 7 & 1 \\ 24 & 10 & 20 & 6 & 9 & 2 & 16 & 19 \\ 23 & 16 & 5 & 19 & 5 & 13 & 17 & 20 \\ 12 & 5 & 12 & 7 & 7 & 19 & 18 & 21 \\ 20 & 17 & 11 & 13 & 15 & 23 & 11 & 3 \\ 4 & 1 & 16 & 17 & 12 & 4 & 3 & 10 \end{pmatrix}$$

Πολλαπλασιάζονται ξεχωριστά με το κλειδί και προκύπτουν οι επόμενοι δυο 8×8 πίνακες :

$$A_1 = \begin{pmatrix} 1558 & 1712 & 486 & 1423 & 1736 & 1392 & 871 & 1204 \\ 634 & 705 & 200 & 578 & 700 & 572 & 351 & 500 \\ 224 & 238 & 67 & 205 & 254 & 195 & 128 & 166 \\ 116 & 141 & 39 & 106 & 126 & 113 & 61 & 100 \\ 772 & 1089 & 1211 & 702 & 873 & 1393 & 1109 & 1319 \\ 308 & 440 & 484 & 279 & 358 & 559 & 460 & 539 \\ 114 & 155 & 178 & 105 & 121 & 203 & 153 & 189 \\ 53 & 84 & 88 & 46 & 74 & 101 & 93 & 100 \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 1720 & 1578 & 1222 & 1284 & 1283 & 806 & 934 & 1129 \\ 699 & 640 & 500 & 510 & 513 & 326 & 388 & 472 \\ 248 & 227 & 171 & 192 & 188 & 118 & 128 & 154 \\ 127 & 120 & 99 & 87 & 93 & 58 & 79 & 96 \\ 1460 & 947 & 938 & 1147 & 810 & 1538 & 1325 & 1392 \\ 583 & 376 & 388 & 461 & 333 & 625 & 534 & 562 \\ 216 & 141 & 129 & 167 & 112 & 220 & 194 & 204 \\ 103 & 66 & 79 & 83 & 68 & 120 & 96 & 9 \end{pmatrix}$$

Κρυπτογραφούνται ξεχωριστά

$$C_1 = \begin{pmatrix} 22 & 176 & 230 & 143 & 200 & 112 & 103 & 180 \\ 122 & 193 & 200 & 66 & 188 & 60 & 95 & 244 \\ 224 & 238 & 67 & 205 & 254 & 195 & 128 & 166 \\ 116 & 141 & 39 & 106 & 126 & 113 & 61 & 100 \\ 4 & 65 & 187 & 190 & 105 & 113 & 85 & 39 \\ 52 & 184 & 228 & 23 & 102 & 47 & 204 & 27 \\ 114 & 155 & 178 & 105 & 121 & 203 & 153 & 189 \\ 53 & 84 & 88 & 46 & 74 & 101 & 93 & 100 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 184 & 42 & 198 & 4 & 3 & 38 & 166 & 105 \\ 187 & 128 & 244 & 254 & 1 & 70 & 132 & 216 \\ 248 & 227 & 171 & 192 & 188 & 118 & 128 & 154 \\ 127 & 120 & 99 & 87 & 93 & 58 & 79 & 96 \\ 180 & 179 & 170 & 123 & 42 & 2 & 45 & 112 \\ 71 & 120 & 132 & 205 & 77 & 113 & 22 & 50 \\ 216 & 141 & 129 & 167 & 112 & 220 & 194 & 204 \\ 103 & 66 & 79 & 83 & 68 & 120 & 96 & 99 \end{pmatrix}$$

Τέλος, τοποθετούνται σε έναν 16×8 σύνθετο πίνακα

$$C=\begin{pmatrix} 22 & 176 & 230 & 143 & 200 & 112 & 103 & 180 \\ 122 & 193 & 200 & 66 & 188 & 60 & 95 & 244 \\ 224 & 238 & 67 & 205 & 254 & 195 & 128 & 166 \\ 116 & 141 & 39 & 106 & 126 & 113 & 61 & 100 \\ 4 & 65 & 187 & 190 & 105 & 113 & 85 & 39 \\ 52 & 184 & 228 & 23 & 102 & 47 & 204 & 27 \\ 114 & 155 & 178 & 105 & 121 & 203 & 153 & 189 \\ 53 & 84 & 88 & 46 & 74 & 101 & 93 & 100 \\ 184 & 42 & 198 & 4 & 3 & 38 & 166 & 105 \\ 187 & 128 & 244 & 254 & 1 & 70 & 132 & 216 \\ 248 & 227 & 171 & 192 & 188 & 118 & 128 & 154 \\ 127 & 120 & 99 & 87 & 93 & 58 & 79 & 96 \\ 180 & 179 & 170 & 123 & 42 & 2 & 45 & 112 \\ 71 & 120 & 132 & 205 & 77 & 113 & 22 & 50 \\ 216 & 141 & 129 & 167 & 112 & 220 & 194 & 204 \\ 103 & 66 & 79 & 83 & 68 & 120 & 96 & 99 \end{pmatrix}$$

2.1.4 Υλοποίηση Αλγορίθμου Αποκρυπτογράφησης μη τετραγωνικού πίνακα με βάρη

Με παρόμοιο τρόπο, όπως ο αλγόριθμος που αναπτύχθηκε στην Υποενότητα 2.1.3, λειτουργεί και ο συγκεκριμένος αλγόριθμος. Υπολογίζει σε πόσους υποπίνακες έχει χωριστεί ο αρχικός πίνακας. Χωρίζει τον πίνακα C σε όσους υποπίνακες είχε χωριστεί και ο αρχικός πίνακας $I1$.

Στη συνέχεια δημιουργείται ένας καινούριος πίνακας από τον κάθε υποπίνακα ξεχωριστά, χρησιμοποιώντας την εξίσωση:

$$R=\frac{1}{\det M}\left(adjM\right)J$$

Έπειτα πραγματοποιείται η πράξη της αποκρυπτογράφησης σε κάθε πίνακα $R \bmod B$. Τέλος ενώνονται όλοι οι πίνακες σε έναν E, ο οποίος είναι ο ίδιος με τον αρχικό $I1$.

Παράδειγμα 2.4

Να γίνει η αποκρυπτογράφηση του πίνακα C, ο οποίος κρυπτογραφήθηκε στο Παράδειγμα 2.3.

Αρχικά χωρίζεται σε υποπίνακες

$$J_1 = \begin{pmatrix} 22 & 176 & 230 & 143 & 200 & 112 & 103 & 180 \\ 122 & 193 & 200 & 66 & 188 & 60 & 95 & 244 \\ 224 & 238 & 67 & 205 & 254 & 195 & 128 & 166 \\ 116 & 141 & 39 & 106 & 126 & 113 & 61 & 100 \\ 4 & 65 & 187 & 190 & 105 & 113 & 85 & 39 \\ 52 & 184 & 228 & 23 & 102 & 47 & 204 & 27 \\ 114 & 155 & 178 & 105 & 121 & 203 & 153 & 189 \\ 53 & 84 & 88 & 46 & 74 & 101 & 93 & 100 \end{pmatrix}$$

$$J_2 = \begin{pmatrix} 184 & 42 & 198 & 4 & 3 & 38 & 166 & 105 \\ 187 & 128 & 244 & 254 & 1 & 70 & 132 & 216 \\ 248 & 227 & 171 & 192 & 188 & 118 & 128 & 154 \\ 127 & 120 & 99 & 87 & 93 & 58 & 79 & 96 \\ 180 & 179 & 170 & 123 & 42 & 2 & 45 & 112 \\ 71 & 120 & 132 & 205 & 77 & 113 & 22 & 50 \\ 216 & 141 & 129 & 167 & 112 & 220 & 194 & 204 \\ 103 & 66 & 79 & 83 & 68 & 120 & 96 & 99 \end{pmatrix}$$

Έπειτα γίνεται η πράξη της αποκρυπτογράφησης και προκύπτουν οι ακόλουθοι 8×8 πίνακες

$$E_1 = \begin{pmatrix} 20 & 11 & 7 & 18 & 22 & 9 & 14 & 6 \\ 22 & 22 & 2 & 19 & 24 & 20 & 12 & 22 \\ 4 & 20 & 3 & 7 & 14 & 15 & 1 & 4 \\ 22 & 24 & 20 & 17 & 4 & 14 & 9 & 20 \\ 16 & 16 & 17 & 16 & 4 & 23 & 4 & 13 \\ 3 & 1 & 8 & 4 & 7 & 7 & 2 & 24 \\ 7 & 21 & 23 & 3 & 21 & 19 & 8 & 2 \\ 14 & 23 & 1 & 12 & 7 & 19 & 13 & 11 \end{pmatrix}$$

$$E_2 = \begin{pmatrix} 23 & 17 & 11 & 24 & 20 & 10 & 4 & 3 \\ 24 & 19 & 10 & 9 & 6 & 14 & 15 & 24 \\ 4 & 18 & 19 & 15 & 23 & 2 & 7 & 1 \\ 24 & 10 & 20 & 6 & 9 & 2 & 16 & 19 \\ 23 & 16 & 5 & 19 & 5 & 13 & 17 & 20 \\ 12 & 5 & 12 & 7 & 7 & 19 & 18 & 21 \\ 20 & 17 & 11 & 13 & 15 & 23 & 11 & 3 \\ 4 & 1 & 16 & 17 & 12 & 4 & 3 & 10 \end{pmatrix}$$

Τέλος, οι πίνακες $E1$ και $E2$ τοποθετούνται σε έναν 16×8 σύνθετο πίνακα τον ακόλουθο:

$$E = I1 = \begin{pmatrix} 20 & 11 & 7 & 18 & 22 & 9 & 14 & 6 \\ 22 & 22 & 2 & 19 & 24 & 20 & 12 & 22 \\ 4 & 20 & 3 & 7 & 14 & 15 & 1 & 4 \\ 22 & 24 & 20 & 17 & 4 & 14 & 9 & 20 \\ 16 & 16 & 17 & 16 & 4 & 23 & 4 & 13 \\ 3 & 1 & 8 & 4 & 7 & 7 & 20 & 24 \\ 7 & 21 & 23 & 3 & 21 & 19 & 8 & 2 \\ 14 & 23 & 1 & 12 & 7 & 19 & 13 & 11 \\ 23 & 17 & 11 & 24 & 20 & 10 & 4 & 3 \\ 24 & 19 & 10 & 9 & 6 & 14 & 15 & 24 \\ 4 & 18 & 19 & 15 & 23 & 2 & 7 & 1 \\ 24 & 10 & 20 & 6 & 9 & 2 & 16 & 19 \\ 23 & 16 & 5 & 19 & 5 & 13 & 17 & 20 \\ 12 & 5 & 12 & 7 & 7 & 19 & 18 & 21 \\ 20 & 17 & 11 & 13 & 15 & 23 & 11 & 3 \\ 4 & 1 & 16 & 17 & 12 & 4 & 3 & 10 \end{pmatrix}$$

2.1.5 Υλοποίηση Αλγορίθμου Κρυπτογράφησης μη τεραγωνικού πίνακα με Βάρη ($2^η$ περίπτωση)

Έστω ένας $m \times n$ πίνακας και $p = \gcd(m,n)$ να είναι ο μέγιστος κοινός διαιρέτης των διαστάσεων του πίνακα, στη συγκεκριμένη περίπτωση δεν χρειάζεται να γνωρίζουμε ποια πλευρά είναι μεγαλύτερη.

Στη συνέχεια όπως και στους προηγούμενους αλγόριθμους δημιουργείται ο πίνακας Q, ο οποίος υψώνεται σε μια δύναμη, που δίνεται στην είσοδο για να δημιουργηθεί το κλειδί. Η βασική διαφορά είναι ότι οι υποπίνακες που δημιουργούνται είναι τετραγωνικοί με διαστάσεις $p \times p$. Στη συνέχεια οι υποπίνακες κρυπτογραφούνται ο καθένας ξεχωριστά και κατόπιν συνθέτονται σε έναν πίνακα.

Σημείωση

Συνθέτονται οι πίνακες σε δύο στάδια, πρώτα συνθέτονται οι τετραγωνικοί αριστερά – δεξιά ξεχωριστά και στη συνέχεια πάνω – κάτω.

Παράδειγμα 2.5

Έστω ότι στην είσοδο είναι $t = 4, k = 4$ και

$$I1 = \begin{pmatrix} 3 & 6 & 17 & 12 & 7 & 16 & 16 & 23 \\ 7 & 17 & 1 & 1 & 19 & 23 & 10 & 16 \\ 4 & 7 & 15 & 5 & 5 & 6 & 21 & 12 \\ 7 & 17 & 10 & 18 & 7 & 18 & 20 & 16 \\ 11 & 17 & 22 & 12 & 3 & 6 & 7 & 14 \\ 13 & 2 & 1 & 4 & 14 & 3 & 15 & 16 \\ 11 & 7 & 12 & 9 & 17 & 15 & 14 & 14 \\ 22 & 6 & 11 & 15 & 14 & 11 & 13 & 18 \\ 13 & 17 & 12 & 5 & 11 & 12 & 21 & 13 \\ 23 & 21 & 19 & 18 & 16 & 16 & 7 & 24 \\ 16 & 9 & 8 & 6 & 16 & 19 & 8 & 6 \\ 23 & 19 & 19 & 23 & 17 & 9 & 3 & 3 \end{pmatrix}$$

Ο τυχαίος πίνακας με τα βάρη είναι $barh = \begin{pmatrix} 2 & 3 & 3 \end{pmatrix}$.

Εφόσον $p = \gcd(m,n) = \gcd(12,8) = 4$, καταλαβαίνουμε ότι ο γενικευμένος πίνακας Fibonacci μπορεί να επιλεγεί ως εξής :

$$Q_4(2,3,3,1)=\begin{pmatrix}2&3&3&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix}$$

Ο Y θα έχει διαστάσεις $\gcd(12,8)/k$ στη συγκεκριμένη περίπτωση, επειδή $\gcd(12,8)=4$ και $k=4$, $Y=1$

Άρα

$$Q=Q_4(2,3,3,1)=\begin{pmatrix}2&3&3&1\\1&0&0&0\\0&1&0&0\\0&0&1&0\end{pmatrix} \quad \text{και} \quad M=Q^t=\begin{pmatrix}74&92&76&23\\23&28&23&7\\7&9&7&2\\2&3&3&1\end{pmatrix}$$

Στη συνέχεια διαμερίζεται ο πίνακας $I1$ σε 6 υποπίνακες 4×4

$$J_1=\begin{pmatrix}3&6&17&12\\7&17&1&1\\4&7&15&5\\7&17&10&18\end{pmatrix}, J_2=\begin{pmatrix}7&16&16&23\\19&23&10&16\\5&6&21&12\\7&18&20&16\end{pmatrix}$$

Τους κρυπτογραφούμε ξεχωριστά

$$C_1=\begin{pmatrix}51&115&160&238\\150&126&66&33\\126&22&253&164\\46&101&92&60\end{pmatrix}, \quad C_2=\begin{pmatrix}247&74&64&102\\89&252&247&85\\13&141&133&165\\93&137&145&146\end{pmatrix}$$

και κατόπιν θεωρούμε τον ακόλουθο σύνθετο πίνακα :

$$C_{12}=\begin{pmatrix}C_1 & C_2\end{pmatrix}=\begin{pmatrix}51&115&160&238&247&74&64&102\\150&126&66&33&89&252&247&85\\126&22&253&164&13&141&133&165\\46&101&92&60&93&137&145&146\end{pmatrix}$$

Στη συνέχεια, γίνεται η ίδια διαδικασία και για τους υπόλοιπους 4 πίνακες

$$J_3=\begin{pmatrix}11&17&22&12\\13&2&1&4\\11&7&12&9\\22&6&11&15\end{pmatrix}, \quad J_4=\begin{pmatrix}3&6&7&14\\14&3&15&16\\17&15&14&14\\14&11&13&18\end{pmatrix}$$

$$C_3 = \begin{pmatrix} 24 & 64 & 69 & 237 \\ 0 & 138 & 119 & 188 \\ 59 & 198 & 13 & 213 \\ 116 & 67 & 94 & 78 \end{pmatrix}, \quad C_4 = \begin{pmatrix} 52 & 65 & 189 & 146 \\ 182 & 132 & 226 & 194 \\ 38 & 196 & 52 & 120 \\ 113 & 77 & 114 & 136 \end{pmatrix}$$

$$C_{34} = \begin{pmatrix} C_3 & C_4 \end{pmatrix} = \begin{pmatrix} 24 & 64 & 69 & 237 & 52 & 65 & 189 & 146 \\ 0 & 138 & 119 & 188 & 182 & 132 & 226 & 194 \\ 59 & 198 & 13 & 213 & 38 & 196 & 52 & 120 \\ 116 & 67 & 94 & 78 & 113 & 77 & 114 & 136 \end{pmatrix}$$

$$J_5 = \begin{pmatrix} 13 & 17 & 12 & 5 \\ 23 & 21 & 19 & 18 \\ 16 & 9 & 8 & 6 \\ 23 & 19 & 19 & 23 \end{pmatrix}, J_6 = \begin{pmatrix} 11 & 12 & 21 & 13 \\ 16 & 16 & 7 & 24 \\ 16 & 19 & 8 & 6 \\ 17 & 9 & 3 & 3 \end{pmatrix}$$

$$C_5 = \begin{pmatrix} 215 & 215 & 97 & 195 \\ 192 & 39 & 101 & 150 \\ 200 & 153 & 93 & 29 \\ 166 & 143 & 124 & 105 \end{pmatrix}, C_6 = \begin{pmatrix} 53 & 171 & 59 & 111 \\ 164 & 200 & 116 & 106 \\ 111 & 123 & 16 & 99 \\ 135 & 138 & 90 & 119 \end{pmatrix}$$

$$C_{56} = \begin{pmatrix} C_5 & C_6 \end{pmatrix} = \begin{pmatrix} 215 & 215 & 97 & 195 & 53 & 171 & 59 & 111 \\ 192 & 39 & 101 & 150 & 164 & 200 & 116 & 106 \\ 200 & 153 & 93 & 29 & 111 & 123 & 16 & 99 \\ 166 & 143 & 124 & 105 & 135 & 138 & 90 & 119 \end{pmatrix}$$

Τέλος, οι 3 τελευταίοι πίνακες C_{12}, C_{34}, C_{56} συνθέτονται σε έναν ενιαίο πίνακα C άπο πάνω προς τα κάτω, ως εξής:

$$C_{123456} = \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \\ C_5 & C_6 \end{pmatrix} :=$$

$$C_{123456} = \begin{pmatrix} C_1 & C_2 \\ C_3 & C_4 \\ C_5 & C_6 \end{pmatrix} := C = \begin{pmatrix} 51 & 115 & 160 & 238 & 247 & 74 & 64 & 102 \\ 150 & 126 & 66 & 33 & 89 & 252 & 247 & 85 \\ 126 & 22 & 253 & 164 & 13 & 141 & 133 & 165 \\ 46 & 101 & 92 & 60 & 93 & 137 & 145 & 146 \\ 24 & 64 & 69 & 237 & 52 & 65 & 189 & 146 \\ 0 & 138 & 119 & 188 & 182 & 132 & 226 & 194 \\ 59 & 198 & 13 & 213 & 38 & 196 & 52 & 120 \\ 116 & 67 & 94 & 78 & 113 & 77 & 114 & 136 \\ 215 & 215 & 97 & 195 & 53 & 171 & 59 & 111 \\ 192 & 39 & 101 & 150 & 164 & 200 & 116 & 106 \\ 200 & 153 & 93 & 29 & 111 & 123 & 16 & 99 \\ 166 & 143 & 124 & 105 & 135 & 138 & 90 & 119 \end{pmatrix}$$

2.1.6 Υλοποίηση Αλγορίθμου Αποκρυπτογράφησης η τεραγωνικού πίνακα με βάρη

Διαμερίζεται ο κρυπτογραφημένος πίνακας σε ίσους υποπίνακες τετραγωνικούς, όπως και προηγουμένως. Αποκρυπτογραφείται, όπως και στην Υποενότητα 2.2.2, και στη συνέχεια συνθέτονται οι αποκρυπτογραφημένοι πίνακες, όπως αυτό πραγματοποιήθηκε προηγούμενα με τους κρυπτογραφημένους πίνακες, (βλέπε Υποενότητα 2.2.3).

Παράδειγμα 2.6

Διαμερίζεται ο πίνακας που προέκυψε από το προηγούμενο Παράδειγμα 2.5

$$C_{123456} = C = \begin{pmatrix} 51 & 115 & 160 & 238 & 247 & 74 & 64 & 102 \\ 150 & 126 & 66 & 33 & 89 & 252 & 247 & 85 \\ 126 & 22 & 253 & 164 & 13 & 141 & 133 & 165 \\ 46 & 101 & 92 & 60 & 93 & 137 & 145 & 146 \\ 24 & 64 & 69 & 237 & 52 & 65 & 189 & 146 \\ 0 & 138 & 119 & 188 & 182 & 132 & 226 & 194 \\ 59 & 198 & 13 & 213 & 38 & 196 & 52 & 120 \\ 116 & 67 & 94 & 78 & 113 & 77 & 114 & 136 \\ 215 & 215 & 97 & 195 & 53 & 171 & 59 & 111 \\ 192 & 39 & 101 & 150 & 164 & 200 & 116 & 106 \\ 200 & 153 & 93 & 29 & 111 & 123 & 16 & 99 \\ 166 & 143 & 124 & 105 & 135 & 138 & 90 & 119 \end{pmatrix}$$

$$J_1 = \begin{pmatrix} 51 & 115 & 160 & 238 \\ 150 & 126 & 66 & 33 \\ 126 & 22 & 253 & 164 \\ 46 & 101 & 92 & 60 \end{pmatrix}, \quad J_2 = \begin{pmatrix} 247 & 74 & 64 & 102 \\ 89 & 252 & 247 & 85 \\ 13 & 141 & 133 & 165 \\ 93 & 137 & 145 & 146 \end{pmatrix},$$

$$J_3 = \begin{pmatrix} 24 & 64 & 69 & 237 \\ 0 & 138 & 119 & 188 \\ 59 & 198 & 13 & 213 \\ 116 & 67 & 94 & 78 \end{pmatrix}, \quad J_4 = \begin{pmatrix} 52 & 65 & 189 & 146 \\ 182 & 132 & 226 & 194 \\ 38 & 196 & 52 & 120 \\ 113 & 77 & 114 & 136 \end{pmatrix},$$

$$J_5 = \begin{pmatrix} 215 & 215 & 97 & 195 \\ 192 & 39 & 101 & 150 \\ 200 & 153 & 93 & 29 \\ 166 & 143 & 124 & 105 \end{pmatrix}, \quad J_6 = \begin{pmatrix} 53 & 171 & 59 & 111 \\ 164 & 200 & 116 & 106 \\ 111 & 123 & 16 & 99 \\ 135 & 138 & 90 & 119 \end{pmatrix}$$

Έπειτα πολλαπλασιάζονται με το κλειδί ξεχωριστά $A = M \cdot J$, στη συνέχεια γίνεται η πράξη του Hill

$$E = \left(\left(\det M \right)^{-1} \left(\text{adj } M \right) J \right) \bmod B$$

$$A_1 = \begin{pmatrix} 28208 & 24097 & 39256 & 34492 \\ 8593 & 7386 & 11991 & 10590 \\ 2681 & 2295 & 3669 & 3231 \\ 976 & 775 & 1369 & 1127 \end{pmatrix}, \quad E_1 = \begin{pmatrix} 3 & 6 & 17 & 12 \\ 7 & 17 & 1 & 1 \\ 4 & 7 & 15 & 5 \\ 7 & 17 & 10 & 18 \end{pmatrix}$$

$$A_2 = \begin{pmatrix} 29593 & 42527 & 40903 & 31266 \\ 9123 & 12960 & 12462 & 9543 \\ 2807 & 4047 & 3892 & 2926 \\ 893 & 1464 & 1413 & 1100 \end{pmatrix}, \quad E_2 = \begin{pmatrix} 7 & 16 & 16 & 23 \\ 19 & 23 & 10 & 16 \\ 5 & 6 & 21 & 12 \\ 7 & 18 & 20 & 16 \end{pmatrix}$$

και συνθέτονται οι δύο πίνακες E_1, E_2 σε έναν 4×8 όπως στη συνέχεια :

$$E_{12} = \begin{pmatrix} 3 & 6 & 17 & 12 & 7 & 16 & 16 & 23 \\ 7 & 17 & 1 & 1 & 19 & 23 & 10 & 16 \\ 4 & 7 & 15 & 5 & 5 & 6 & 21 & 12 \\ 7 & 17 & 10 & 18 & 7 & 18 & 20 & 16 \end{pmatrix}$$

$$A_3 = \begin{pmatrix} 8928 & 34021 & 19204 & 52816 \\ 2721 & 10359 & 5876 & 16160 \\ 813 & 3210 & 1833 & 4998 \\ 341 & 1203 & 628 & 1755 \end{pmatrix}, E_3 = \begin{pmatrix} 11 & 17 & 22 & 12 \\ 13 & 2 & 1 & 4 \\ 11 & 7 & 12 & 9 \\ 22 & 6 & 11 & 15 \end{pmatrix}$$

$$A_4 = \begin{pmatrix} 26079 & 33621 & 41352 & 40900 \\ 7957 & 10238 & 12669 & 12502 \\ 2494 & 3169 & 3949 & 3880 \\ 877 & 1191 & 1326 & 1370 \end{pmatrix}, E_4 = \begin{pmatrix} 3 & 6 & 7 & 14 \\ 14 & 3 & 15 & 16 \\ 17 & 15 & 14 & 14 \\ 14 & 11 & 13 & 18 \end{pmatrix}$$

$$E_{34} = \begin{pmatrix} 11 & 17 & 22 & 12 & 3 & 6 & 7 & 14 \\ 13 & 2 & 1 & 4 & 14 & 3 & 15 & 16 \\ 11 & 7 & 12 & 9 & 17 & 15 & 14 & 14 \\ 22 & 6 & 11 & 15 & 14 & 11 & 13 & 18 \end{pmatrix}$$

$$A_5 = \begin{pmatrix} 52592 & 34415 & 26390 & 32849 \\ 16083 & 10557 & 8066 & 10087 \\ 4965 & 3213 & 2487 & 3128 \\ 1772 & 1149 & 900 & 1032 \end{pmatrix}, \quad E_5 = \begin{pmatrix} 13 & 17 & 12 & 5 \\ 23 & 21 & 19 & 18 \\ 16 & 9 & 8 & 6 \\ 23 & 19 & 19 & 23 \end{pmatrix}$$

$$A_6 = \begin{pmatrix} 30551 & 43576 & 18324 & 28227 \\ 9309 & 13328 & 5603 & 8631 \\ 2894 & 4134 & 1749 & 2662 \\ 1066 & 1449 & 604 & 956 \end{pmatrix}, \quad E_6 = \begin{pmatrix} 11 & 12 & 21 & 13 \\ 16 & 16 & 7 & 24 \\ 16 & 19 & 8 & 6 \\ 17 & 9 & 3 & 3 \end{pmatrix}$$

$$E_{56} = \begin{pmatrix} 13 & 17 & 12 & 5 & 11 & 12 & 21 & 13 \\ 23 & 21 & 19 & 18 & 16 & 16 & 7 & 24 \\ 16 & 9 & 8 & 6 & 16 & 19 & 8 & 6 \\ 23 & 19 & 19 & 23 & 17 & 9 & 3 & 3 \end{pmatrix}$$

Τέλος, συνθέτονται οι πίνακες E_{12}, E_{34}, E_{56} σε έναν 12×8 πίνακα E άπο πάνω προς τα κάτω, ως εξής:

$$E_{123456} = \begin{pmatrix} E_{12} \\ E_{34} \\ E_{56} \end{pmatrix} := E = I1 = \left(\begin{array}{cccc:cccc} 3 & 6 & 17 & 12 & 7 & 16 & 16 & 23 \\ 7 & 17 & 1 & 1 & 19 & 23 & 10 & 16 \\ 4 & 7 & 15 & 5 & 5 & 6 & 21 & 12 \\ 7 & 17 & 10 & 18 & 7 & 18 & 20 & 16 \\ \hdashline 11 & 17 & 22 & 12 & 3 & 6 & 7 & 14 \\ 13 & 2 & 1 & 4 & 14 & 3 & 15 & 16 \\ 11 & 7 & 12 & 9 & 17 & 15 & 14 & 14 \\ 22 & 6 & 11 & 15 & 14 & 11 & 13 & 18 \\ \hdashline 13 & 17 & 12 & 5 & 11 & 12 & 21 & 13 \\ 23 & 21 & 19 & 18 & 16 & 16 & 7 & 24 \\ 16 & 9 & 8 & 6 & 16 & 19 & 8 & 6 \\ 23 & 19 & 19 & 23 & 17 & 9 & 3 & 3 \end{array}\right)$$

2.2 Κρυπταλγόριθμος με αναδιάταξη

Στο συγκεκριμένο κεφάλαιο αναπτύσσεται ένας άλλος αλγόριθμος κρυπτογράφησης, στον οποίο υπάρχουν ομοιότητες με αυτούς του προηγούμενου κεφαλαίου, με τη διαφορά ότι πρώτα διαταράσσονται τα στοιχεία του πίνακα και κατόπιν κρυπτογραφούνται, γεγονός που καθιστά ακόμα πιο δύσκολο σε κάποιον, που δεν γνωρίζει το κλειδί, να σπάσει τον αλγόριθμο και να διαβάσει τα δεδομένα που ανταλάσσονται (Κώδικας B5, B6).

2.2.1 Συναρτήσεις shuffling και deshuffling

Για το συγκεκριμένο κεφάλαιο δημιουργήθηκαν δυο νέες συναρτήσεις: η μία αναδιατάσσει τα στοιχεία του πίνακα (shuffling.m) και η δεύτερη κάνει την αντίστροφη διαδικασία, επιστρέφοντας τα στοιχεία στην αρχική τους θέση (deshuffling.m) (Κώδικας B4).

Η συνάρτηση shuffling δέχεται σαν είσοδο τον πίνακα που χρειάζεται να κρυπτογραφηθεί και έναν θετικό ακέραιο k. Αρχικά υπολογίζονται οι διαστάσεις του αρχικού πίνακα $m \times n$ και δημιουργούνται νέες μεταβλητές, οι οποίες είναι οι διαστάσεις των υποπινάκων, που χρησιμοποιούνται $r_w = n/k$ και $cl_w = m/k$. Τέλος, ο αριθμός των πινάκων που δημιουργούνται υπολογίζεται από

$$number\ of\ buckets = \frac{n \cdot m}{k \cdot k}.$$

Έπειτα γίνεται αναδιάταξη με την εξίσωση μέσα σε μία επανάληψη με την οποία ο αλγόριθμος προσπελαύνει το κάθε στοιχείο του αρχικού πίνακα στην i-οστή γραμμή και j-οστή στήλη

$$b = (i \bmod r_w) \cdot cl_w + (j \bmod cl_w) + 1 \qquad (18)$$

Με την εξίσωση (18) υπολογίζεται το *bucket* στο οποίο πρέπει να καταχωρηθεί το συγκεκριμένο στοιχείο

$$buckets(ii(b), jj(b), b) = I1(i, j) \qquad (19)$$

Με την εξίσωση (19) εκχωρείται το κάθε στοιχείο του αρχικού πίνακα στο αντίστοιχο bucket (b).

Συγχρόνως ελέγχουμε αν έχουμε ξεπεράσει το k που έχει δόθεί και ανάλογα αλλάζουμε σειρά.

Με αντίστοιχο τρόπο γίνεται η σύνθεση των υποπινάκων με την συνάρτηση deshuffling. Η αλλαγή που υπάρχει είναι στην βασική εξίσωση μέσα στην επανάληψη, αντί να παίρνει από τον αρχικό πίνακα τα στοιχεία και να δημιουργεί υποπίνακες, παίρνει απο τους υποπίνακες στοιχεία και δημιουργεί τον αρχικό πίνακα.

Παράδειγμα 2.7

Έστω $k=2$ και ότι ο αρχικός πίνακας, που πρέπει να αναδιαταχθούν τα στοιχεία του είναι $I1=\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{pmatrix}$.

Παρατηρούμε ότι ο πίνακας $I1$ έχει διαστάσεις 4×4, άρα υπάρχουν 4 υποπίνακες διάστασεων 2×2 οι ακόλουθοι

$$bucket1=\begin{pmatrix} 6 & 8 \\ 14 & 16 \end{pmatrix},\ bucket2=\begin{pmatrix} 5 & 7 \\ 13 & 15 \end{pmatrix},\ bucket3=\begin{pmatrix} 2 & 4 \\ 10 & 12 \end{pmatrix},\ bucket4=\begin{pmatrix} 1 & 3 \\ 9 & 11 \end{pmatrix}$$

Ο πίνακας $Cbuckets_{2\times 2\times 4}$ είναι η σύνθεση των παραπάνω πινάκων. Η αντίστροφη διαδικασία δημιουργεί τον πίνακα $I1$.

2.2.2 Αλγόριθμος κρυπτογράφησης με αναδιάταξη

Στη συγκεκριμένη ενότητα περιγράφεται ο αλγόριθμος κρυπτογράφησης, στον οποίο χρησιμοποιείεται η μέθοδος της αναδιάταξης (Κώδικας B5)

Αρχικά όπως και στους υπόλοιπους αλγόριθμους χρειάζεται να γνωρίζουμε τις διαστάσεις του αρχικού πίνακα, έπειτα χρησιμοποιείται η συνάρτηση, που υπάρχει στην Ενότητα 3.1 (shuffling) και βγάζει ως αποτέλεσμα τους διάφορους υποπίνακες με τα αναδιαταγμένα στοιχεία. Στη συνέχεια βρίσκει με τον ίδιο τρόπο, όπως στο Κεφάλαιο 2 τους πίνακες Q, Q_k, Y και το κλειδί M.

Έπειτα δημιουργούνται πίνακες πολλαπλασιάζοντας το κλειδί με τον κάθε υποπίνακα που έχει προκύψει απο την συνάρτηση shuffling, χρειάζεται και ένας πίνακας Β ο οποίος θα έχει ίσες διαστάσεις με τους υποπίνακες. Έπειτα πραγματοποιείται η πράξη της κρυπτογράφησης του κάθε πίνακα, δηλαδή $A \bmod B$ και τους αποθηκεύει όλους σε έναν πίνακα. Τέλος καλεί την συνάρτηση deshuffling

Παράδειγμα 2.8

Έστω ότι δέχεται ως είσοδο $k=8, t=4$ και

$$I1=\begin{pmatrix} 14 & 23 & 9 & 11 & 22 & 11 & 14 & 18 & 22 & 10 & 5 & 1 & 1 & 15 & 24 & 6 \\ 17 & 18 & 19 & 16 & 17 & 8 & 12 & 16 & 12 & 22 & 6 & 18 & 17 & 8 & 4 & 2 \\ 9 & 23 & 3 & 4 & 6 & 7 & 7 & 5 & 11 & 1 & 24 & 21 & 23 & 20 & 3 & 15 \\ 2 & 13 & 15 & 11 & 19 & 6 & 24 & 23 & 8 & 21 & 15 & 3 & 21 & 20 & 22 & 19 \\ 11 & 6 & 11 & 16 & 7 & 23 & 5 & 14 & 2 & 7 & 8 & 1 & 3 & 19 & 12 & 13 \\ 2 & 7 & 18 & 20 & 7 & 21 & 21 & 7 & 19 & 7 & 24 & 15 & 9 & 9 & 21 & 1 \\ 18 & 19 & 7 & 8 & 1 & 10 & 1 & 14 & 4 & 12 & 22 & 15 & 6 & 2 & 20 & 24 \\ 1 & 24 & 3 & 10 & 9 & 12 & 8 & 22 & 9 & 18 & 5 & 13 & 14 & 18 & 5 & 13 \end{pmatrix}$$

Χρησιμοποιείται η συνάρτηση shuffling και προκύπτουν οι εξής πίνακες

$$bucket_1=\begin{pmatrix} 23 & 11 & 11 & 18 & 10 & 1 & 15 & 6 \\ 18 & 16 & 8 & 16 & 22 & 18 & 8 & 2 \\ 23 & 4 & 7 & 5 & 1 & 21 & 20 & 15 \\ 13 & 11 & 6 & 23 & 21 & 3 & 20 & 19 \\ 6 & 16 & 23 & 14 & 7 & 1 & 19 & 13 \\ 7 & 20 & 21 & 7 & 7 & 15 & 9 & 1 \\ 19 & 8 & 10 & 14 & 12 & 15 & 2 & 24 \\ 24 & 10 & 12 & 22 & 18 & 13 & 18 & 13 \end{pmatrix}$$

$$bucket_2=\begin{pmatrix} 14 & 9 & 22 & 14 & 22 & 5 & 1 & 24 \\ 17 & 19 & 17 & 12 & 12 & 6 & 17 & 4 \\ 9 & 3 & 6 & 7 & 11 & 24 & 23 & 3 \\ 2 & 15 & 19 & 24 & 8 & 15 & 21 & 22 \\ 11 & 11 & 7 & 5 & 2 & 8 & 3 & 12 \\ 2 & 18 & 7 & 21 & 19 & 24 & 9 & 21 \\ 18 & 7 & 1 & 1 & 4 & 22 & 6 & 20 \\ 1 & 3 & 9 & 8 & 9 & 5 & 14 & 5 \end{pmatrix}$$

Ο τυχαίος πίνακας με τα βάρη είναι $barh = \begin{pmatrix} 2 & 1 & 4 \end{pmatrix}$

Άρα ο $Q_4(2,1,4,1) = \begin{pmatrix} 2 & 1 & 4 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}$ και $Y = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ διότι $n/k = 2$

Το αποτέλεσμα του γινομένου Kronecker ανάμεσα στον $Q_4(2,1,4,1)$ Q_k και Y είναι :

$$Q = \begin{pmatrix} 2 & 1 & 4 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 1 & 4 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

Άρα

$$M = Q^4 = \begin{pmatrix} 46 & 38 & 69 & 16 & 0 & 0 & 0 & 0 \\ 16 & 14 & 22 & 5 & 0 & 0 & 0 & 0 \\ 5 & 6 & 9 & 2 & 0 & 0 & 0 & 0 \\ 2 & 1 & 4 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 46 & 38 & 69 & 16 \\ 0 & 0 & 0 & 0 & 16 & 14 & 22 & 5 \\ 0 & 0 & 0 & 0 & 5 & 6 & 9 & 2 \\ 0 & 0 & 0 & 0 & 2 & 1 & 4 & 1 \end{pmatrix}$$

Στη συνέχεια δημιουργούνται δύο πίνακες απο τον πολλαπλασιασμό των δυο υποπινάκων που παράχθηκαν από την συνάρτηση shuffling

$A_1 = M \cdot bucket_1$

$$= \begin{pmatrix} 3537 & 1566 & 1389 & 2149 & 1701 & 2227 & 2694 & 1691 \\ 1191 & 543 & 472 & 737 & 595 & 745 & 892 & 549 \\ 456 & 209 & 178 & 277 & 233 & 308 & 343 & 215 \\ 169 & 65 & 64 & 95 & 67 & 107 & 138 & 93 \\ 2237 & 2208 & 2738 & 2228 & 1704 & 1859 & 1642 & 2500 \\ 732 & 762 & 942 & 740 & 564 & 621 & 564 & 815 \\ 291 & 292 & 355 & 282 & 221 & 256 & 203 & 313 \\ 119 & 94 & 119 & 113 & 87 & 90 & 73 & 136 \end{pmatrix}$$

$$A_2 = M \cdot bucket_2$$

$$= \begin{pmatrix} 1943 & 1583 & 2376 & 1967 & 2355 & 2354 & 2615 & 1815 \\ 670 & 551 & 817 & 666 & 802 & 767 & 865 & 616 \\ 257 & 216 & 304 & 253 & 297 & 307 & 356 & 215 \\ 83 & 64 & 104 & 92 & 108 & 127 & 132 & 86 \\ 1840 & 1721 & 801 & 1225 & 1234 & 2878 & 1118 & 2810 \\ 605 & 597 & 277 & 436 & 431 & 973 & 376 & 951 \\ 231 & 232 & 104 & 176 & 178 & 392 & 151 & 376 \\ 97 & 71 & 34 & 43 & 48 & 133 & 53 & 130 \end{pmatrix}$$

Στη συνέχεια κρυπτογραφούνται ξεχωριστά και προκύπτουν οι 8×8 πίνακες

$$C_1 = \begin{pmatrix} 209 & 30 & 109 & 101 & 165 & 179 & 134 & 155 \\ 167 & 31 & 216 & 225 & 83 & 233 & 124 & 37 \\ 200 & 209 & 178 & 21 & 233 & 52 & 87 & 215 \\ 169 & 65 & 64 & 95 & 67 & 107 & 138 & 93 \\ 189 & 160 & 178 & 180 & 168 & 67 & 106 & 196 \\ 220 & 250 & 174 & 228 & 52 & 109 & 52 & 47 \\ 35 & 36 & 99 & 26 & 221 & 0 & 203 & 57 \\ 119 & 94 & 119 & 113 & 87 & 90 & 73 & 136 \end{pmatrix}$$

$$C_2 = \begin{pmatrix} 151 & 47 & 72 & 175 & 51 & 50 & 55 & 23 \\ 158 & 39 & 49 & 154 & 34 & 255 & 97 & 104 \\ 1 & 216 & 48 & 253 & 41 & 51 & 100 & 215 \\ 83 & 64 & 104 & 92 & 108 & 127 & 132 & 86 \\ 48 & 185 & 33 & 201 & 210 & 62 & 94 & 250 \\ 93 & 85 & 21 & 180 & 175 & 205 & 120 & 183 \\ 231 & 232 & 104 & 176 & 178 & 136 & 151 & 120 \\ 97 & 71 & 34 & 43 & 48 & 133 & 53 & 130 \end{pmatrix}$$

Τέλος χρησιμοποιείται η συνάρτηση deshuffling και δημιουργείται ένας 8×16 πίνακας

$$C_{12} = C = \begin{pmatrix} 151 & 209 & 47 & 30 & 72 & 109 & 175 & 101 & 51 & 165 & 50 & 179 & 55 & 134 & 23 & 155 \\ 158 & 167 & 39 & 31 & 49 & 216 & 154 & 225 & 34 & 83 & 255 & 233 & 97 & 124 & 104 & 37 \\ 1 & 200 & 216 & 209 & 48 & 178 & 253 & 21 & 41 & 233 & 51 & 52 & 100 & 87 & 215 & 215 \\ 83 & 169 & 64 & 65 & 104 & 64 & 92 & 95 & 108 & 67 & 127 & 107 & 132 & 138 & 86 & 93 \\ 48 & 189 & 185 & 160 & 33 & 178 & 201 & 180 & 210 & 168 & 62 & 67 & 94 & 106 & 250 & 196 \\ 93 & 220 & 85 & 250 & 21 & 174 & 180 & 228 & 175 & 52 & 205 & 109 & 120 & 52 & 183 & 47 \\ 231 & 35 & 232 & 36 & 104 & 99 & 176 & 26 & 178 & 221 & 136 & 0 & 151 & 203 & 120 & 57 \\ 97 & 119 & 71 & 94 & 34 & 119 & 43 & 113 & 48 & 87 & 133 & 90 & 53 & 73 & 130 & 136 \end{pmatrix}$$

2.2.3 Αλγόριθμος αποκρυπτογράφησης με αναδιάταξη

Στη συγκεκριμένη υποενότητα παρουσιάζεται ο πίνακας αποκρυπτογράφησης με τη μέθοδο του αναδιάταξης.

Στο συγκεκριμένο αλγόριθμο χρησιμοποιείται η συνάρτηση decodewithshuffling.m (Κώδικας Β6) για να επαναφέρει τον αναδιαταγμένο κρυπτογραφημένο πίνακα στην αρχική του μορφή. Όπως και στην Υποενότητα 3.2 χρησιμοποιούνται και εδώ οι συναρτήσεις shuffling και deshuffling.

Αρχικά καθορίζοται οι διαστάσεις του κρυπτογραφημένου πίνακα, κατόπιν καλείται η συνάρτηση shuffling.m για να δημιουργηθούν οι ανακατεμμένοι υποπίνακες όπως και στον αλγόριθμο της κρυπτογράφησης. Στη συνέχεια εφαρμόζεται η πράξη της αποκρυπτογράφησης του αλγορίθμου Hill σε κάθε υποπίνακα ξεχωριστά

$$\left(\det M\right)^{-1} \cdot \operatorname{adj} M \cdot \text{buckets} \bmod B .$$

Τέλος καλείται η συνάρτηση deshuffling.m και δημιουργείται ο αρχικός πίνακας $I1$ μετά τη σύνθεση των αποκρυπτογραφημένων υποπινάκων.

Παράδειγμα 2.9

Χρησιμοποιείται τον πίνακα που δημιουργήθηκε στο Παράδειγμα 2.8.

$$C_{12} = C = \begin{pmatrix} 151 & 209 & 47 & 30 & 72 & 109 & 175 & 101 & 51 & 165 & 50 & 179 & 55 & 134 & 23 & 155 \\ 158 & 167 & 39 & 31 & 49 & 216 & 154 & 225 & 34 & 83 & 255 & 233 & 97 & 124 & 104 & 37 \\ 1 & 200 & 216 & 209 & 48 & 178 & 253 & 21 & 41 & 233 & 51 & 52 & 100 & 87 & 215 & 215 \\ 83 & 169 & 64 & 65 & 104 & 64 & 92 & 95 & 108 & 67 & 127 & 107 & 132 & 138 & 86 & 93 \\ 48 & 189 & 185 & 160 & 33 & 178 & 201 & 180 & 210 & 168 & 62 & 67 & 94 & 106 & 250 & 196 \\ 93 & 220 & 85 & 250 & 21 & 174 & 180 & 228 & 175 & 52 & 205 & 109 & 120 & 52 & 183 & 47 \\ 231 & 35 & 232 & 36 & 104 & 99 & 176 & 26 & 178 & 221 & 136 & 0 & 151 & 203 & 120 & 57 \\ 97 & 119 & 71 & 94 & 34 & 119 & 43 & 113 & 48 & 87 & 133 & 90 & 53 & 73 & 130 & 136 \end{pmatrix}$$

Δημιουργείται ένας 8×8 πίνακας $B = \begin{pmatrix} 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \\ 256 & 256 & 256 & 256 & 256 & 256 & 256 & 256 \end{pmatrix}$

Στη συνέχεια υπολογίζεται $E = (\det M)^{-1} \cdot \text{adj}M \cdot \text{buckets} \bmod B$ και προκύπτουν οι πίνακες:

$$E_1 = \begin{pmatrix} 23 & 11 & 11 & 18 & 10 & 1 & 15 & 6 \\ 18 & 16 & 8 & 16 & 22 & 18 & 8 & 2 \\ 23 & 4 & 7 & 5 & 1 & 21 & 20 & 15 \\ 13 & 11 & 6 & 23 & 21 & 3 & 20 & 19 \\ 6 & 16 & 23 & 14 & 7 & 1 & 19 & 13 \\ 7 & 20 & 21 & 7 & 7 & 15 & 9 & 1 \\ 19 & 8 & 10 & 14 & 12 & 15 & 2 & 24 \\ 24 & 10 & 12 & 22 & 18 & 13 & 18 & 13 \end{pmatrix} \quad E_2 = \begin{pmatrix} 14 & 9 & 22 & 14 & 22 & 5 & 1 & 24 \\ 17 & 19 & 17 & 12 & 12 & 6 & 17 & 4 \\ 9 & 3 & 6 & 7 & 11 & 24 & 23 & 3 \\ 2 & 15 & 19 & 24 & 8 & 15 & 21 & 22 \\ 11 & 11 & 7 & 5 & 2 & 8 & 3 & 12 \\ 2 & 18 & 7 & 21 & 19 & 24 & 9 & 21 \\ 18 & 7 & 1 & 1 & 4 & 22 & 6 & 20 \\ 1 & 3 & 9 & 8 & 9 & 5 & 14 & 5 \end{pmatrix}$$

Στο τέλος του αλγόριθμου καλείται η συνάρτηση deshuffling και παράγεται ο αρχικός πίνακας:

$$E = I1 = \begin{pmatrix} 14 & 23 & 9 & 11 & 22 & 11 & 14 & 18 & 22 & 10 & 5 & 1 & 1 & 15 & 24 & 6 \\ 17 & 18 & 19 & 16 & 17 & 8 & 12 & 16 & 12 & 22 & 6 & 18 & 17 & 8 & 4 & 2 \\ 9 & 23 & 3 & 4 & 6 & 7 & 7 & 5 & 11 & 1 & 24 & 21 & 23 & 20 & 3 & 15 \\ 2 & 13 & 15 & 11 & 19 & 6 & 24 & 23 & 8 & 21 & 15 & 3 & 21 & 20 & 22 & 19 \\ 11 & 6 & 11 & 16 & 7 & 23 & 5 & 14 & 2 & 7 & 8 & 1 & 3 & 19 & 12 & 13 \\ 2 & 7 & 18 & 20 & 7 & 21 & 21 & 7 & 19 & 7 & 24 & 15 & 9 & 9 & 21 & 1 \\ 18 & 19 & 7 & 8 & 1 & 10 & 1 & 14 & 4 & 12 & 22 & 15 & 6 & 2 & 20 & 24 \\ 1 & 24 & 3 & 10 & 9 & 12 & 8 & 22 & 9 & 18 & 5 & 13 & 14 & 18 & 5 & 13 \end{pmatrix}$$

2.3 Μέτρα σύγκρισης ποιότητας κρυπτογράφησης

Στη συγκεκριμένη υποενότητα παρουσιάζονται κάποια μέτρα σύγκρισης των κρυπταλγορίθμων. Τα βασικά μέτρα που χρησιμοποιούνται στη βιβλιογραφία [35] είναι ο Correlation Coefficient Measuring (CC), ο Irregular Deviation (ID) και ο Condition Number (CN).

- Εδώ θεωρούμε ότι ένας $m \times n$ πίνακας μπορεί να αντιστοιχηθεί σε πίνακα στήλη διάστασης $N \times 1$ με $N = mn$. Έχοντας τις τιμές δύο παρατηρήσεων $X = \begin{pmatrix} x_1 & x_2 & \cdots & x_N \end{pmatrix}^t$ και $Y = \begin{pmatrix} y_1 & y_2 & \cdots & y_N \end{pmatrix}^t$ ορίζεται ο συντελεστής συσχέτισης (Correlation Coefficient) αυτών ως

$$CC = \frac{\operatorname{cov}(X,Y)}{\sigma_X \sigma_Y} = \frac{\sum_{i=1}^{N} (x_i - E(X))(y_i - E(Y))}{\sqrt{\sum_{i=1}^{N} (x_i - E(X))^2} \sqrt{\sum_{i=1}^{N} (y_i - E(Y))^2}}$$

όπου $E(X), E(Y)$ σημειώνει τη μέση τιμή της κάθε παρατήρησης X, Y, αντίστοιχα.

Αν ο συντελεστής συσχέτισης είναι ίσος με τη μονάδα, τότε οι παρατηρήσεις X, Y είναι «εξαρτημένες», που σημαίνει ότι οι δύο πίνακες, από όπου προέκυψαν οι παρατηρήσεις X, Y, είναι ίσοι ή έχουν ανάλογα στοιχεία, εάν ο συντελεστής συσχέτισης είναι ίσος με -1, τότε ο ένας πίνακας έχει αντίθετες τιμές από τον άλλον. Όσο πιο κοντά στο 0 είναι ο συντελεστής συσχέτισης, τόσο πιο διαφορετικά είναι τα στοιχεία των X, Y.

Εδώ θεωρούμε ότι ο αρχικός $m \times n$ πίνακας I παράγει τον X και ο κρυπτογραφημένος πίνακας παράγει τον Y. Σύμφωνα με τα παραπάνω, όσο πιο κοντά είναι ο συντελεστής συσχέτισης στο 0, τόσο πιο διαφορετικά είναι ο αρχικός πίνακας από τον κρυπτογραφημένο, άρα είναι καλύτερη η κρυπτογράφηση. Αν ο συντελεστής συσχέτισης είναι κοντά στην απόλυτη μονάδα, τότε οι δύο πίνακες είναι «σχεδόν όμοιοι», οπότε η κρυπτογράφηση δεν είναι καλή.

- Η διαδικασία υπολογισμού του δεύτερου μέτρου (ID) είναι η εξής:

Αρχικά υπολογίζεται η απόλυτη διαφορά $D=|I-J|$ μεταξύ των τιμών του αρχικού πίνακα I και του κρυπτογραφημένου J.

Έπειτα υπολογίζεται το ιστόγραμμα του D.

Υπολογίζεται ο μέσος όρος των pixels του ιστογράμματος $DC=\frac{1}{256}\sum_{1}^{256}h_i$

Αφαιρείται ο μέσος όρος από το ιστόγραμμα και σημειώνεται η απόλυτη τιμή από το αποτέλεσμα $AC(i)=|H(i)-DC|$

Τέλος υπολογίζεται η περιοχή κάτω από την απόλυτη τιμή AC, η οποία προκύπτει από το άθροισμα $ID=\sum_{i=1}^{256}AC(i)$.

Όσο πιο μικρή είναι η τιμή του ID τόσο καλύτερη είναι η κρυπτογράφηση.

- Ο δείκτης κατάστασης (Condition Number) ενός τετραγωνικού συμμετρικού πίνακα $A\in M_n(\mathbb{F})$ θετικά ορισμένου (με θετικές πραγματικές ιδιοτιμές) δίνεται ως εξής

$$CN=\sqrt{\frac{\lambda_{max}}{\lambda_{min}}},$$

όπου λ_{max} είναι η μέγιστη ιδιοτιμή και λ_{min} η ελάχιστη ιδιοτιμή του πίνακα A.

Ο δείκτης κατάστασης ενός πίνακα $A\in M_n(\mathbb{F})$ είναι ένα μέτρο που δείχνει πόσο «κοντά» βρίσκεται ο πίνακας στην ιδιότητα της αντιστρεψιμότητάς του. Από τις πιο γνωστές ιδιότητες του δείκτη κατάστασης έχουμε να αναφέρουμε :

i. Ο δείκτης κατάστασης του μοναδιαίου πίνακα είναι ίσος με 1.
ii. Για το δείκτη κατάστασης ενός πίνακα $A\in M_n(\mathbb{F})$ ισχύει $cond(A)\geq 1$.
iii. Αν $A,B\in M_n(\mathbb{F})$, τότε $cond(AB)\leq cond(A)\cdot cond(B)$.
iv. Αν ο πίνακας $A\in M_n(\mathbb{F})$ δεν είναι αντιστρέψιμος, τότε $cond(A)$ είναι πολύ μεγάλος αριθμός δηλαδή τείνει στο άπειρο.
v. Αν ο δείκτης κατάστασης ενός πίνακα $A\in M_n(\mathbb{F})$ είναι πολύ μεγάλος αριθμός αυτό σημαίνει ότι για το βαθμό r του πίνακα A ισχύει $r(A)=r<n$, το οποίο επιπρόσθετα σημαίνει ότι οι στήλες/γραμμές είναι γραμμικά εξαρτημένα διανύσματα.

Σχόλιο 2.2

Εδώ για να υπολογίσουμε το δείκτη κατάστασης θεωρούμε ότι ο αρχικός $m \times n$ πίνακας I αντιστοιχεί σε έναν πίνακα γραμμή $\tilde{I}$ διάστασης $1 \times mn$. Επειδή ο κρυπτογραφημένος πίνακας C έχει τις ίδιες διαστάσεις με τον αρχικό πίνακα, προφανώς ο κρυπτογραφημένος C αντιστοιχεί σε έναν πίνακα γραμμή $\tilde{C}$ διάστασης διάστασης $1 \times mn$.

Θεωρούμε το $2 \times mn$ σύνθετο πίνακα $\tilde{K} = \begin{pmatrix} \tilde{I} \\ \tilde{C} \end{pmatrix}$.

Στη συνέχεια υπολογίζεται ο 2×2 πίνακας $K = \tilde{K}\tilde{K}'$, ο οποίος είναι συμμετρικός και θετικά ημιορισμένος, (δηλαδή, έχει θετικές ιδιοτιμές) .

Υπολογίζονται οι ιδιοτιμές του K , οι οποίες είναι μη αρνητικοί αριθμοί, οπότε επιλέγουμε από αυτές τη μεγαλύτερη ως λ_{max} και τη μικρότερη ως λ_{min} προκειμένου να υπολογίσουμε το δείκτη κατάστασης του πίνακα K.

Αν ο δείκτης κατάστασης του πίνακα K είναι πολύ μεγάλος αριθμός αυτό σημαίνει ότι οι γραμμές είναι γραμμικά εξαρτημένα διανύσματα, άρα ο αρχικός πίνακας και ο κρυπτογραφημένος είναι «σχεδόν όμοιοι», οπότε η κρυπτογράφηση δεν είναι καλή.

Αντίθετα, αν ο δείκτης κατάστασης του πίνακα K είναι κοντά στη μονάδα αυτό σημαίνει ότι οι γραμμές είναι ανεξάρτητα (διαφορετικά) διανύσματα, άρα η κρυπτογράφηση είναι καλή.

Παράδειγμα 2.10

Στο συγκεκρίμενο παράδειγμα χρησιμοποιούνται δύο τετραγωνικές εικόνες διαστάσεων 64x64 και κρυπτογραφούνται με το ίδιο κλειδί με τους δύο διαφορετικούς αλγορίθμους. Οι εικόνες είναι πίνακες με τιμές από 0...255. Έπειτα χρησιμοποιώντας τα παραπάνω μέτρα σύγκρισης σημειώνονται τα αποτελέσματα.

Το πειράματα τρέχουν και στις δυο περιπτώσεις για $k = 8$, $t = 10$ και βάρη $c_1 = 2, c_2 = 1, c_3 = 3, c_4 = 5, c_5 = 6, c_6 = 7, c_7 = 4, c_8 = 1$:

$$Q_8(c_1,c_2,c_3,c_4,c_5,c_6,c_7,c_8)=\begin{pmatrix}2&1&3&5&6&7&4&1\\1&0&0&0&0&0&0&0\\0&1&0&0&0&0&0&0\\0&0&1&0&0&0&0&0\\0&0&0&1&0&0&0&0\\0&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0\\0&0&0&0&0&0&1&0\end{pmatrix}$$

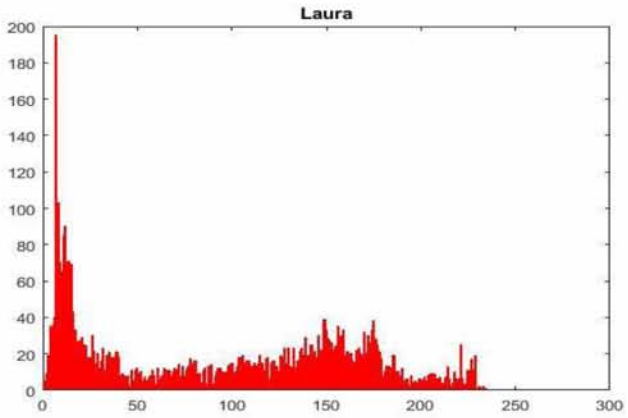
Οι εικόνες που χρησιμοποιούνται για το παράδειγμα είναι ασπρόμαυρες και εμφανίζονται στο Σχήμα 2.1.

Laura.gif

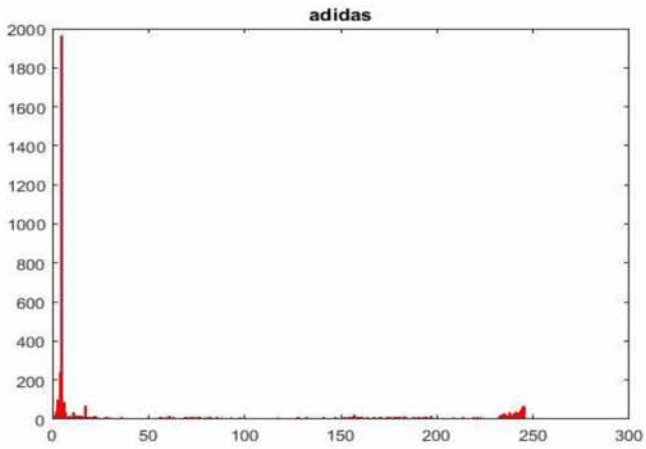
adidas.gif

Σχήμα 2.1: Δύο ασπρόμαυρες εικόνες του Παραδείγματος 2.4

Χρησιμοποιώντας MATLAB, σχεδιάζονται τα ιστογράμματα των εικόνων του Σχήματος 2.1, τα οποία παρουσιάζονται στο Σχήμα 2.2.



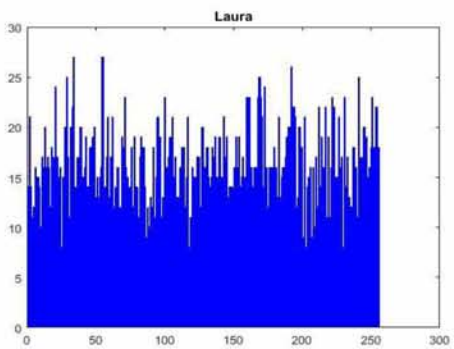
(a)

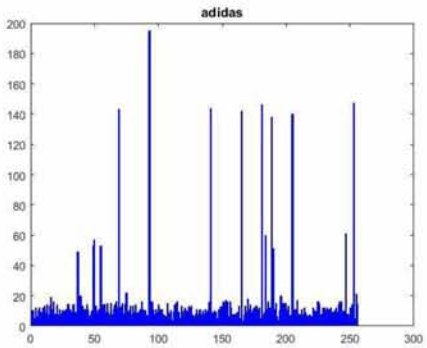


(b)

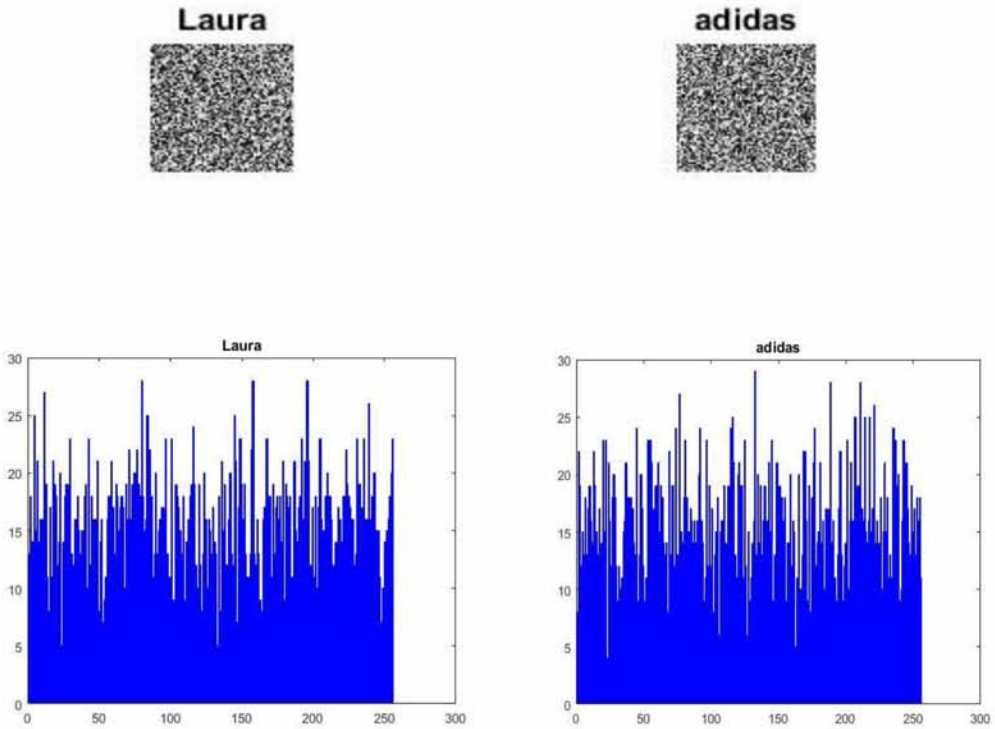
Σχήμα 2.2: Ιστογράμματα- (a): Laura (b):-adidas

Στα Σχήματα 2.3 και 2.4 παρουσιάζονται οι κρυπτογραφημένες εικόνες του Σχήματος 2.1 και τα ιστογράμματα τους χρησιμοποιώντας τον αλγόριθμο χωρίς/με αναδιάταξη.





Σχήμα 2.3: Κρυπτογραφημένες εικόνες με αλγόριθμο χωρίς αναδιάταξη και τα αντίστοιχα ιστογράμματά τους



Σχήμα 2.3: Κρυπτογραφημένες εικόνες με αλγόριθμο με αναδιάταξη και τα αντίστοιχα ιστογράμματά τους

Τέλος στον Πίνακα 2.1 παρουσιάζονται συνολικά τα αποτελέσματα των μέτρων Κρυπτογράφησης

Πίνακας 2.1: Πίνακας Σύγκριση Αλγορίθμων

cipher	Χωρίς αναδιάταξη			Με αναδιάταξη		
	CC	ID	CN	CC	ID	CN
Laura	0.0090	2142	2.4388	0.0028	2078	2.4709
Adidas	0.1119	2930	1.9265	0.0030	1124	1.9214

Παράδειγμα 2.11

Στο συγκεκριμένο παράδειγμα χρησιμοποιείται η εικόνα Laura.gif για τυχαία κλειδιά Q_8^{10} την πρώτη φόρα το εύρος των βαρών $([c_1, c_2, c_3 ... c_{k-1}] = [1...4]$ και τη δεύτερη $[c_1, c_2, .., c_{k-1}] = [1...7]$

Πίνακας 2.2: Πίνακας διαφορετικών βαρών

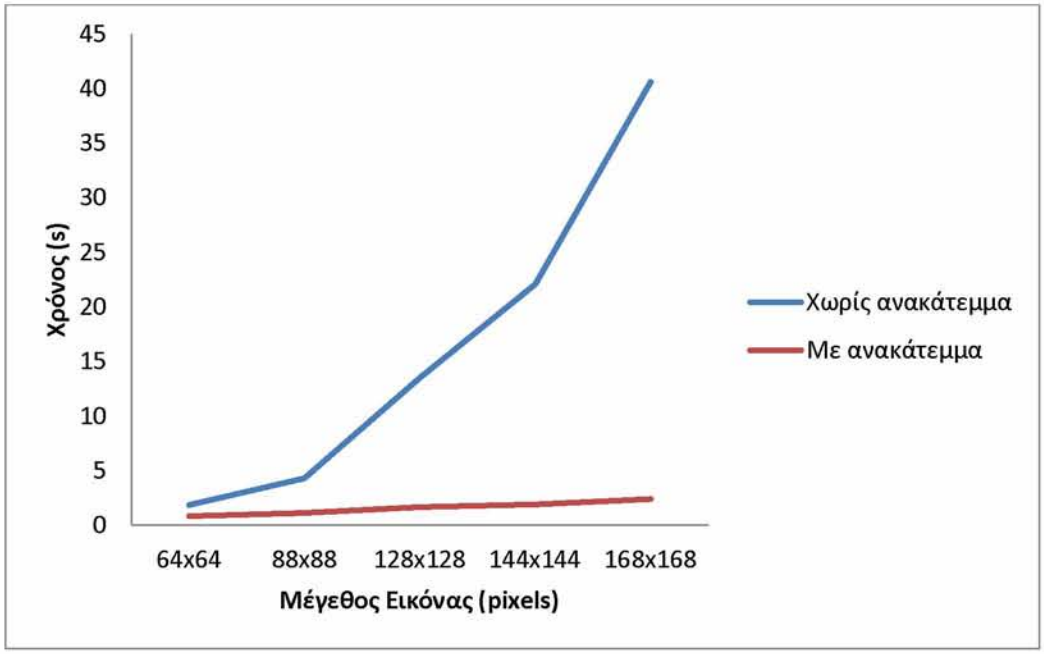
Laura	CC	ID	CN
[1...4]	0.0022	2103	2.4325
[1...7]	0.0015	2071	2.4293

Στον Πίνακα 2.3 παρουσιάζονται τα αποτέλεσματα των μέτρων για κλειδιά διαφορετικού μεγέθους αλλά ίδιας δύναμης.

Πίνακας 2.3: Πίνακας διαφορετικού μεγέθους κλειδιών

Laura	CC	ID	CN
Q_{16}^{16}	0.0002	2080	2.4254
Q_8^{16}	0.0019	2118	2.4277
Q_4^{16}	0.0024	2626	2.4298

Στον Πίνακα 2.4 απεικονίζεται ο χρόνος εκτέλεσης ξεχωριστά του κάθε αλγορίθμου για εικόνες διαφορετικών διαστάσεων.



Πίνακας 2.4: Χρόνοι Εκτέλεσης των αλγορίθμων

Συμπεράσματα

Στην παρούσα πτυχιακή δημιουργήθηκαν αλγόριθμοι για την κρυπτογράφηση και την αποκρυπτογράφηση πινάκων με τη χρήση γενικευμένων πινάκων Fibonacci και του κρυπταλγορίθμου του Hill. Στην αρχή παρατέθηκαν κάποιες βασικές έννοιες, οι οποίες είναι απαραίτητες για την κατανόηση των αλγορίθμων που δημιουργήθηκαν. Στη συνέχεια παρουσιάζεται ο κάθε αλγόριθμος αναλυτικά.

Ο πρώτος αλγόριθμος, που περιγράφεται (βλέπε, Κεφάλαιο 2.1), κρυπτογραφεί έναν πίνακα A, χρησιμοποιώντας τον πίνακα ή τον διαιρεί σε τετραγωνικούς υποπίνακες. Ο δεύτερος αλγόριθμος, που περιγράφεται (βλέπε, Κεφάλαιο 2.2), αναδιατάσσει τα στοιχεία του πίνακα και τα αποθηκεύει σε μικρότερους υποπίνακες, τους οποίους κρυπτογραφεί και αποκρυπτογραφεί ξεχωριστά.

Για την αξιολόγηση των προτεινόμενων αλγορίθμων πραγματοποιήθηκαν μετρήσεις με ασπρόμαυρες εικόνες, των οποίων τα pixels αντιπροσωπεύονται από τιμές στο διάστημα [0-255].

Παρατηρώντας τα αποτελέσματα φαίνεται ότι η προσθήκη της αναδιάταξης βελτιώνει την κρυπτογράφηση. Συγκεκριμένα, σε εικόνες που έχουν φόντο ένα χρώμα, δηλαδή, έχουν πολλά pixels με την ίδια τιμή σε πολύ κοντινές θέσεις, ο αλγόριθμος με την αναδιάταξη κρυπτογραφεί καλύτερα, όπως είναι εμφανές από τα ιστογράμματα και τις κρυπτογραφημένες εικόνες.

Επίσης όσο μεγαλύτερες είναι οι διαστάσεις του πίνακα-κλειδί τόσο καλύτερη είναι η κρυπτογράφηση, αυτό γίνεται διότι υπάρχει ο περιορισμός $k \leq t$, και όσο αυξάνεται το μέγεθος του κλειδιού, τόσο αυξάνεται και η δύναμη στην οποία υψώνεται ο πίνακας-κλειδί (Πίνακας 2.3.3). Επίσης όσο αυξάνονται οι τιμές των βαρών τόσο πιο καλή είναι η κρυπτογράφηση (Πίνακας 2.3.2).

Τέλος ο αλγόριθμος με την αναδιάταξη είναι αρκετά πιο γρήγορος (Πίνακας 2.3.4), διότι κρυπτογραφεί τα μέρη της εικόνας (Κεφάλαιο 2.3.1), αντίθετα ο άλλος αλγόριθμος κρυπτογραφεί όλη την εικόνα ή μεγάλα μέρη της, οπότε όσο μεγαλώνει η εικόνα μεγαλώνει και το κλειδί.

Υλοποιώντας τους αλγορίθμους παρατηρούμε ότι αν οι αλγόριθμοι δεχτούν ως είσοδο πίνακες με βάρη που να είναι μεγάλοι αριθμοί, τότε στην αποκρυπτογράφηση

προκύπτει πίνακας με στοιχεία που τείνουν στο μηδέν (Σχόλιο 2.1). Ένα ανοιχτό πρόβλημα που χρειάζεται περαιτέρω μελέτη είναι η βελτίωση του αλγορίθμου σχετικά με τα όρια των τιμών των βαρών και των δυνάμεων του κλειδιού, που δέχεται ως είσοδο για να αντιμετωπιστεί το πρόβλημα που αναφέρθηκε, (Σχόλιο 2.1). Όλοι οι αλγόριθμοι υλοποιούνται σε MATLAB 2015.

Βιβλιογραφία

[1] Maria Adam, Powers of the generalized 2-Fibonacci matrices. *Applied Mathematics & Bioinformatics*, vol.6(3), (2016), 145-154.

[2] Adam M., & Assimakis N., k-step Fibonacci sequences and Fibonacci matrices. *Journal of Discrete Mathematical Sciences & Cryptography*, (2014).

[3] Adam, M., Assimakis, N., & Tziallas, G., Generalized k, m-step Fibonacci sequences and matrices, Int. Journal of Algebraic Hyperstructures and its Applications, vol. 2(1), (2015), 125-134.

[4] Laub, A. J. *Matrix Analysis for Scientists and Engineers,SIAM*, 2005.

[5] Xudan Fu and Xia Zhou, On matrices related with Fibonacci and Lucas numbers, *Applied Mathematics and Computation*, 200, (2008), 96-100.

[6] Erdal Karaduman, *on determinants of matrices with general Fibonacci numbers entries*, Applied Mathematics and Computation, vol. 167, (2005), 670 -676.

[7] John Ivie, A general Q-matrix, *The Fibonacci Quarterly*, vol. 10(3), (1972), 255-264.

[8] G. - Y. Lee, S. - G. Lee and H. - G. Shin, On the k – Generalized Fibonacci matrix Q_k , *LinearAlgebra and its Applications*, vol. 251, 73 - 88.

[9] (1997),M. Mishra, P. Mishra, M. C. Adhikary and S. Kumar, Image encryption using Fibonacci – Lucas transformation, *International Journal on Cryptography and Information Security* (IJCIS), vol. 2(3), (September, 2012), 131 – 141.

[10] Σ. Γκριτζάλης, Σ. Κ. Κάτσικα και Δ. Γκριτζάλης, *Ασφάλεια Δικτύων Υπολογιστών*, Παπασωτηρίου, Αθήνα, 2003.

[11] L. – P. Shao, Z. Qin, H. – L.Gao and X. – C. Heng, 2D triangular mappings and their applications in scrambling rectangle image, *Information Technology Journal*, vol. 7(1), 2008, 40 – 47.

[12] The Mathworks Inc. , *The Student edition of* MATLAB, Prentice – Hall, 1997.

[13] Rosen Kenneth, *Elementary Number Theory and its Applications*, fifth edition, Addison – Wesley, 2005, 292.

[14] http://historyoflinearalgebra.weebly.com/lester-s-hill-jdr.html

[15] Άγγελος Ηλίας, *Μελέτη ακολουθίας Fibonacci με άθροισμα k-όρων μετά από m – όρους*, Πτυχιακή εργασία, Λαμία, 2015.

[16] https://www.britannica.com/biography/Leonardo-Pisano

[17] Dan Kalman, Generalized Fibonacci numbers by matrix methods, *The Fibonacci Quarterly,* vol. 22(3), (1984), 204-207.

[18] Mao, Wenbo, *Modern Cryptography: Theory and Practice*, Prentice Hall, 2003.

[19] A. J. Menezes, P. C. V. Oorschot and S. A. Vanstone, *Handbook of applied cryptography,* CRC Press, 1997.

[20] R. Shirey, Internet Security Glossary, Version 2, RFC 4949 (Informational), Aug. 2007, Obsoletes RFC 2828.

[21] M. Burmester, Σ. Γκριτζάλης, Σ. Κάτσικας, Β. Χρυσικόπουλος, *Σύγχρονη Κρυπτογραφία: Θεωρία και Εφαρμογές*, Παπασωτηρίου, Αθήνα, 2011.

[22] Κ. Ε. Πατσάκης, Ε. Χ. Φούντας, Κρυπτογραφία και Εφαρμογές, Τόμος Α, Βαρβαρήγου, Πειραιάς.

[23] M. Mogollon, *Cryptography and security services: mechanisms and applications.* Idea group Inc (IGI), June 2008.

[24] V.I. Arnold and A. Avez, *Ergotic Problems in Classical Mechanics*, New York, 1968.

[25] Ma, Z.G. and S. S. Qiu, *An image cryptosystem based on general cat map*, J. China Inst. Commun., vol. 24, (2003), 51- 57.

[26] Kong, T. and Z. Dan, *A new anti-Arnold transform algorithm,* J. Software, vol. 15, (2004), 1558-1564.

[27] Hong, C. Y. and W. G. Zou, *Digital image scrambling technology based on three dimensions Arnold transform and its period,* J. Nanchang Univ. Nat. Sci., vol. 29, (2005), 619-621.

[28] Wang Z. H. *On the period of 2D Random matrix scrambling transform and its application in image hiding*, Chinese J. Comput., vol. 29, (2006), 2218 - 2225.

[29] Yang, D. L. N. Cai and G. Q. Ni, *Digital image scrambling technology based on the symmetry of Arnold transformation,* J. Beijing Inst. Technol., 15, (2006), 216-220.

[30] Minati Mishra, A. R. Routray, Sunit Kumar, *High Security Image Steganography with modified Arnold's cat map,* IJCA, vol. 37, 9 (2012), 16-20.

[31] Minati Mishra, Sunit Kumar and Subhadra Mishra, *Security Enhanced Image Steganography based on successive Arnold transformation,* Advances in Intelligent and soft computing, vol. 167/2012, (2012), 221-229.

[32] Qi, D. X., J.C. Zou X. Y. Han, *A new class of transform and its application in the image transform covering,* Sci. China(Series E), vol. 43, (2000), 304-312.

Zou, J. C., R. K. Ward and D. X. Qi, *A new digital image scrambling method based on Fibonacci numbers,* Proceedings of the Intenational Symposium on Circuits and Systems, (May 23-26, 2004), Canada, 965-968.

[34] Zou, J.C., R.K. Ward and D.X. Qi, *The generalized Fibonacci transformations and application to image scrambling,* Proceedings of the the IEEE International Conference on Acoustic, Speech and Signal Processing, May 17-21, Canada, (2004), 385-388.

[35] Nawal El-Fishawy and Osama M. Abu Zaid, *Quality of Encryption Measurement of Bitmap Images with RC6, MRC6, and Rijndael Block Cipher Algorithms,* International Journal of Network Security, vol. 5(3), Egypt, 2007, 241-251.

Παράρτημα Α

Ο Lester S.Hill ήταν μαθηματικός στη σύχρονη εποχή. Γεννήθηκε στη Νέα Υόρκη το 1891 και πέθανε στη Νέα Υόρκη το 1961. Σπούδασε στο πανεπιστήμιο της Columbia και απέκτησε το διδακτορικό του από το πανεπιστήμιο του Yale. Αφότου τελείωσε με τις σπουδές συνέχισε να ασχολείται με την εκπαίδευση. Αφιέρωσε τη ζωή του στη διδασκαλία μαθηματικών και αστρονομίας σε 5 διαφορετικά πανεπιστήμια των ΗΠΑ. Επίσης ενεπλάκη με το στρατό και τιμήθηκε για την προσφορά του από την αμερικάνικη κυβέρνηση πριν και κατά τη διάρκεια του Δευτέρου Παγκοσμίου Πολέμου. Ασχολήθηκε με την εφαρμογή ανώτερων μαθηματικών στον τομέα των επικοινωνιών και ανέπτυξε πολλές μεθόδους διόρθωσης λαθών στις επικοινωνίες με τηλέγραφο. Ήταν ένας από τους μεγαλύτερους αντιπροσώπους της κρυπτολογίας (η τέχνη να δημιουργείς και να σπας κώδικες). Το 1929 ανάκαλυψε το γνωστό αλγόριθμο, στον οποίο δόθηκε και το όνομα του, επίσης έφτιαξε μια μηχανή κρυπτογράφησης με αλυσίδες και τροχούς. Σε όλη του τη ζωή χρησιμοποιούσε τις μαθηματικές του γνώσεις για να δημιουργεί και να αποκρυπτογραφεί κρυπτογραφημένα συστήματα. Πέθανε στην ηλικία των 70 από άγνωστη ασθένεια [14].

Ο Fibonacci ή αλλιώς Fibonacci της Πίζας, γεννήθηκε το 1175 και πέθανε μετά το 1240 στην πόλη της Πίζας. Ήταν από τους σπουδαιότερους Ευρωπαίους μαθηματικούς και έμεινε στην ιστορία για τη γνωστή ακολουθία Fibonacci και για κάποιες άλλες μαθηματικές καινοτομίες. Ήταν γιος του Guglielmo Bonacci, για αυτό ονομάστηκε Fibonacci (filius: γιος του Bonacci). Ο πατέρας του ήταν αντιπρόσωπος των εμπόρων της Πίζας στη Βόρεια Αφρική. Έζησε στην πόλη Μπεχάια στη σημερινή Αλγερία. Εκεί σπούδασε λογιστική και έμαθε για το Ινδοαραβικό αριθμητικό σύστημα και τα πλεονεκτήματα του. Το 1202 δημοσιεύει το πρώτο του βιβλίο με το όνομα «Liber Abacci» (βιβλίο των υπολογισμών), μέσα στο οποίο δείχνει πόσο πρακτικό ήταν το αραβικό σύστημα αρίθμησης για εμπορικές συναλλαγές, στον υπολογισμό επιτοκίων ,στις μετατροπές των μέτρων και των σταθμών και σε άλλες εφαρμογές. Ήταν ο πρώτος που εισήγαγε στην Ευρώπη το Ινδοαραβικό συστημα αρίθμησης και μετά την εφεύρεση της τυπογραφίας έγινε ευρέως γνωστό. Το 1240 τιμήθηκε από τη δημοκρατία της Πίζας για τη συνεισφορά του και για τη βοήθεια που προσέφερε στους πολίτες σε θέματα αριθμητικής. Άλλο σημαντικό έργο του ήταν το «Practica Geometriae» το οποίο δημοσιεύθηκε το 1220, μέσα στο οποίο ανάφερει τεχνικές μέτρησης και χωρισμού περιοχών γης, και άλλα πρακτικά θέματα πάνω στη γεωμετρία και την τριγωνομετρία. Άλλα έργα του «Flos», «Liber quadratorum», «Di minor guisa» [16].

Παράρτημα Β

Κώδικας Β1

Ο συγκεκριμένος αλγόριθμος κρυπτογραφεί τετραγωνικό και μη τετραγωνικό πίνακα για τυχαία βάρη χωρίς να αναδιατάσσει τις τιμές του αρχικού πίνακα. Χρησιμοποιείται στο Κεφάλαιο 2.1

```
function [C,Qk,M]=encode(I1,k,t)

%INPUT
%I1=Αρχικός πίνακας
%k=Διάσταση του πίνακα
%t=Δύναμη που υψώνεται το κλειδί
%OUTPUT
%C=κρυπτογραφημένος πίνακας
%Qk=πίνακας Fibonacci
%M=κλειδί

I1 = imread(I1);
figure; imshow(I1);
I1 = double(I1);
[n,m] = size(I1);
barh = randi([1 3],1,k-1);

if n<=m
    r = n/k;
else
    r = m/k;
end

b = 1;
Qk = [barh b; eye(k-1,k-1) zeros(k-1,1)];
dQk = det(Qk);
Y = eye(r);
Q = kron(Y,Qk);
d = det(Q);
M = Q^t;
mkd = gcd(n,m);

if n == m
    A = M*I1;
    B = 256*ones(n,m);
    C = mod(A,B);

elseif mod(m,n) == 0

    numberOfChunks = m/n;
    B = 256*ones(n,n);
    C = [];

    for i = 0:numberOfChunks - 1
        J = I1(:, 1 + i*n:(i+1)*n);
        A = M*J;
        C1 = mod(A,B);
```

```
        C = [C, C1];
    end
    D1=C-I1

elseif mod(n,m)==0

    numberOfChunks = n/m;
    B = 256*ones(m,m);
    C = [];

    for i = 0:numberOfChunks - 1
        J = I1(1 + i*m:(i+1)*m, :);
        A = M*J;
        C1 = mod(A,B);
        C = [C; C1];
    end
    D1 = C-I1

elseif mkd ~= 1
    B = 256*ones(mkd,mkd);
    C = [];
    b = 1;
    Qk = [barh b; eye(k-1,k-1) zeros(k-1,1)];
    dQk = det(Qk);
    Y = eye(mkd/k);
    Q = kron(Y,Qk)
    d = det(Q);
    M = Q^t;

    for i = 1:n/mkd
        Cj=[];
        for j = 1:m/mkd
        J = I1(1 +(i-1)*mkd: i*mkd, 1+(j-1)*mkd : j*mkd);
        A = M*J;
        C1 = mod(A,B);
        Cj = [Cj C1];
        end
        C=[C ; Cj];
    end
    D1 = C - I1;
end
figure;imshow(C,[]);
```

Κώδικας Β2

Ο συγκεκριμένος αλγόριθμος αποκρυπτογράφει τον κρυπτογραφημένο πίνακα που έχει ως έξοδο ο Κώδικας Β1. Χρησιμοποιείται στο Κεφάλαιο 2.1

```
function [E] = decode(C, M)

%INPUT
%C=κρυπτογραφημένος πίνακας
%M=κλειδί
%OUTPUT
%E=αποκρηπτογραφημένος πίνακας

C=double(C);
[n,m] = size(C);
dM = det(M);
dM = round(dM);
g = gcd(dM, 256);
B = 256*ones(n,n);
mkd=gcd(n,m);

if g==1
    if n==m
         R = 1/det(M) * adjoint(M) *C ;
         E=mod(R,B);

    elseif mod(m,n) == 0

        numberOfChunks = m/n;
        B = 256*ones(n,n);
        E = [];

        for i = 0:numberOfChunks - 1
        J = C(:, 1 + i*n:(i+1)*n);
        R = 1/det(M) * adjoint(M) *J ;
        E1=mod(R,B);
        E = [E, E1];
        end

    elseif mod(n,m) == 0

         numberOfChunks = n/m;
         B = 256*ones(m,m);
         E = [];

        for i = 0:numberOfChunks - 1
            J = C(1 + i*m:(i+1)*m, :);
            R = 1/det(M) * adjoint(M) *J ;
            E1=mod(R,B)
            E = [E; E1];
        end

    elseif mkd ~= 1

         B = 256*ones(mkd,mkd);
         E = [];
```

```
        for i = 1:n/mkd

            Ej=[];
            for j = 1:m/mkd
                J = C(1 +(i-1)*mkd: i*mkd, 1+(j-1)*mkd : j*mkd)
                A = M*J
                R = 1/det(M) * adjoint(M) *J
                E1 = mod(R,B)
                Ej = [Ej E1]
            end
            E=[E ; Ej]
        end
    end
end
      E( E > 255) = 0;
      E = int64(E);
    figure;imshow(E, []);
```

Κώδικας Β3

Η συγκεκριμένη συνάρτηση υπολογίζει τον προσαρτημένο πίνακα του κλειδιού.

```
%INPUT
%M = κλειδί
%OUTPUT
%adjo = προσαρτημένος πίνακας του M

function [adjo] = adjoint(M)

[m,n] = size(M);
adjo = zeros(m,n);
%D = zeros(m-1,n-1);
for i = 1:m
    for j = 1:n

      D = [M(1:i-1,1:j-1) M(1:i-1, j+1:n); M(i+1:m,1:j-1)
M(i+1:m,j+1:n)];

        adjo(i,j) = (-1)^(i+j) * det(D) ;

    end
end

adjo = adjo.' ;
```

Κώδικας Β4

Οι συγκεκριμένοι αλγόριθμοι αναδιατάσσουν και ξαναεπαναφέρουν στην αρχική τους μορφή τα στοιχεία ενός πίνακα, Κεφάλαιο 2.3.

```
function [buckets] = shuffling(I1,k)

%INPUT
%I1=πίνακας που θα ανακατευτούν τα στοιχεία του
%k=διάσταση των υποπινάκων
%OUTPUT
%buckets=ο ανακατεμένος πίνακας

I1=imread(I1)
[n,m] = size(I1)
gr_par = n/k;
st_par = m/k;
numberofbuckets = (n*m/(k*k));
buckets = zeros(k,k,numberofbuckets);
ii = ones(1,numberofbuckets);
jj = ones(1,numberofbuckets);

for i = 1:n
    for j = 1:m
        bucket = (mod(i,gr_par)*st_par+mod(j,st_par))+1;
        buckets(ii(bucket),jj(bucket),bucket) = I1(i,j);
        if jj(bucket) < k
            jj(bucket) = jj(bucket) + 1 ;
        else
            ii(bucket) = ii(bucket) + 1 ;
            jj(bucket) = 1 ;
        end
    end
end
```

```
function [Ikrupto]=deshuffling(Cbuckets,n,m,k)

gr_par = n/k;
st_par = m/k;
numberofbuckets=(n*m/(k*k))
buckets = zeros(k,k,numberofbuckets);
ii = ones(1,numberofbuckets);
jj = ones(1,numberofbuckets);

for i = 1:n
    for j = 1:m
        bucket = (mod(i,gr_par)*st_par+mod(j,st_par))+1;
        Ikrupto(i,j)=Cbuckets(ii(bucket),jj(bucket),bucket) ;
        if jj(bucket) < k
            jj(bucket) = jj(bucket) + 1 ;
        else
            ii(bucket) = ii(bucket) + 1 ;
            jj(bucket) = 1 ;
        end
    end
end
```

Κώδικας B5

Ο συγκεκριμένος αλγόριθμος κρυπτογραφεί έναν πίνακα με τη μέθοδο της αναδιάταξης. Διαιρεί την εικόνα σε ίσους πίνακες τετραγωνικούς τους αναδιατάσσει και τους κρυπτογραφεί, Κεφάλαιο 2.3.

```
function [Ikrupto,M]=encodeWithShuffling(I1,k,t)

%INPUT
%I1=Αρχικός πίνακας
%k=Διάσταση του πίνακα
%t=Δύναμη που υψώνεται το κλειδί
%OUTPUT
%Ikrupto2=αποκρυπτογραφημένος πίνακας
%M=κλειδί

%I1=imread(I1);
[g,s] = size(I1)
figure;imshow(I1);
[buckets] = shuffling(I1,8)
I1 = double(I1);
[n,m,numberofbuckets] = size(buckets)
barh = randi([1 4],1,k-1)

r=n/k
b = 1;
Qk = [barh b; eye(k-1,k-1) zeros(k-1,1)]
dQk = det(Qk);
Y = eye(r)
Q = kron(Y,Qk)
d = det(Q)
M = Q^t;

Cbuckets = zeros (n,m,numberofbuckets);
for i = 1 : numberofbuckets

    A = M*buckets(:,:,i);
    B = 256*ones(n,m);
    C = mod(A,B);
    Cbuckets(:,:,i) = C;
end
[Ikrupto]=deshuffling(Cbuckets,g,s,8)
figure;imshow(Ikrupto2,[]);
```

Κώδικας Β6

Ο αλγόριθμος αποκρυπτογραφεί τον πίνακα που προέκυψε από τον Κώδικα Β6.

```
function [Iapokrupto]=decodeWithShuffling(Ikrupto,M)

%INPUT
%Ikrupto=κρυπτογραφημένος πίνακας
%M=κλειδί
%OUTPUT
%Iapokrupto= αποκρυπτογραφημένος πίνακας

[gr,s] = size(Ikrupto)
[buckets] = shuffling(Ikrupto,8);
[n,m,numberofbuckets] = size(buckets);
dM = det(M);
dM = round(dM);
g = gcd(dM, 256);
B=256*ones(n, m);
Ebuckets = zeros (n,m,numberofbuckets);
if g==1
    for i = 1:numberofbuckets
         R = 1/det(M)*adjoint(M)*buckets(:,:,i);
         E=mod(R,B);
         Ebuckets(:,:,i)= E;
    end
end
[Iapokrupto]=deshuffling(Ebuckets,gr,s,8)
figure;imshow(Iapokrupto,[]);
```

Περίληψη

Σκοπός της παρούσας πτυχιακής είναι η ανάπτυξη αλγορίθμων κρυπτογράφησης πινάκων με κλειδί ένα γενικευμένο πίνακα Fibonacci τυχαίων βαρών δυνάμεων και διαστάσεων.

Στην πτυχιακή αναπτύσσονται αλγόριθμοι οι οποίοι κρυπτογραφούν και αποκρυπτογραφούν πίνακες με τη χρήση των γενικευμένων πινάκων Fibonacci και του αλγορίθμου του Hill.

Ο πρώτος αλγόριθμος κρυπτογραφεί έναν πίνακα A, χρησιμοποιώντας τον πίνακα ή διαιρώντας τον σε τετραγωνικούς υποπίνακες. Ο δεύτερος αλγόριθμος αναδιατάσσει τα στοιχεία του πίνακα και τα αποθηκεύει σε μικρότερους υποπίνακες, τους οποίους κρυπτογραφεί και αποκρυπτογραφεί ξεχωριστά.

Επιπλέον, χρησιμοποιήθηκαν κάποια μέτρα σύγκρισης κρυπτογράφησης αλγορίθμων για τη μέτρηση της ποιότητας της κρυπτογράφησης. Ο προτεινόμενος κρυπταλγόριθμος με αναδιάταξη έχει την καλύτερη επίδοση ως προς το χρόνο και την ποιότητα της κρυπτογράφησης.

Όλοι οι αλγόριθμοι υλοποιήθηκαν σε Matlab 2015.

Λέξεις κλειδιά: γενικευμένη ακολουθία Fibonacci, αλγόριθμος Hill, κρυπτογράφηση πίνακα, ασπρόμαυρη εικόνα

Abstract

In this thesis, encoding and decoding codes are proposed using the Hill algorithm and the different powers of the generalized Fibonacci matrices, which are defined by arbitary weights and dimensions as key of algorithm.

The first algorithm encodes a matrix A, using the whole matrix or dividing it in rectangular submatrices. The second algorithm rearranges the values of the matrix A, saves them in other smaller submatrices, encodes, and decodes them individually.

In addition, some metrics are used to evaluate the quality of encryption of the two algorithms. The second algorithm is faster and has a better quality of encryption than the other one.

All the codes were created in MATLAB 2015.

Key words: generalized Fibonacci sequence, Hill cipher, matrix encoding, greyscale image