Υπολογιστική Κρυπτογραφία
1η Σειρά Ασκήσεων

Μαραβίτσας Παναγιώτης
Α.Μ: 03116206

27 Οκτωβρίου 2020

Περιεχόμενα

Άσκηση 1

1.

Η Eve κατάφερε να αποκρυπτογραφήσει τον αλγόριθμο Vigenere χωρίς να διαθέτει το μυστικό κλειδί αφού η κρυπτανάλυσή του είναι αρκετά απλή. Το πρώτο βήμα είναι η εύρεση του μήκους του κλειδιού.

Ο πρώτος τρόπος είναι μέσω της μεθόδου Kasiski. Η μέθοδος αυτή βασίζεται στην παρατήρηση πως αν υπάρχουν επαναλαμβανόμενα μοτίβα στο ciphertext τότε είναι πολύ πιθανό αυτά να προέρχονται από το ίδιο plaintext. Σε αυτή την περίπτωση είναι πολύ πιθανό πως το μήκος της απόστασης μεταξύ των επαναλαμβανόμενων μοτίβων είναι πολλαπλάσιο του μήκους του κλειδιού. Εντοπίζοντας περισσότερα επαναλαμβανόμενα μοτίβα μπορούμε να προσδιορίσουμε με ακόμα μεγαλύτερη βεβαιότητα και το μήκος του κλειδιού. Για κάθε υποψήφιο μήκος κλειδιού k_i, χωρίζουμε το κείμενο σε γραμμές μήκους k_i. Έτσι αν το μήκος κλειδιού που δοκιμάστηκε είναι το σωστό, τότε τα γράμματα που βρίσκονται σε κάθε στήλη έχουν μετατοπιστεί τον ίδιο αριθμό θέσεων, συνεπώς για επαρκώς μεγάλα κείμενα ο δείκτης σύμπτωσης $IC(X) = \sum_{i=0}^{25} \frac{f_i(f_i-1)}{n(n-1)}$ προσεγγίζει το δείκτη σύμπτωσης ενός αγγλικού κειμένου για το οποίο ισχύει ότι $E[IC(X)] \approx 0.065$.

Ο δεύτερος τρόπος να προσδιοριστεί ο το μήκος του κλειδιού είναι με χρήση της σχέσης $k = \frac{E[I_L]-E[I_r]}{E[I_{C_k}]-E[I_r]}$.

Γνωρίζοντας πλέον και το μήκος του κλειδιού και έχοντας χωρίσει το κείμενο σε γραμμές μήκους k αρκεί να μετατοπίσουμε κάθε γραμμή ώστε ο αμοιβαίος δείκτης σύμπτωσης μεταξύ όλων των γραμμών να προσεγγίζει τον δείκτη σύμπτωσης ενός αγγλικού κειμένου. Ο δείκτης αμοιβαίας σύμπτωσης μεταξύ της ολισθημένης n-οστής στήλης και της m-οστής στήλης δίνεται από τη σχέση $IMC(C_{n>>j}, C_m) = \sum_{i=0}^{25} \frac{f_{n>>j}(i)f_m(i)}{|C_n||C_m|}$. Έχοντας σχηματίσει ένα κείμενο με ένα ενιαίο shift μπορούμε να βρούμε το σωστό shift ελέγχοντας τη συχνότητα εμφάνισης του κάθε γράμματος σύμφωνα με την κατανομή των γραμμάτων σε ένα κείμενο της αγγλικής γλώσσας. Για παράδειγμα το συχνότερο γράμμα αντιστοιχεί στο Ε κτλπ.

Η τροποποίηση των κλειδιών με τον αλγόριθμο του Καίσαρα δεν αποτελεί εμπόδιο για την Eve αφού μπορεί να χρησιμοποιήσει ακριβώς την ίδια τεχνική για να αποκρυπτογραφήσει το αρχικό μήνυμα. Το μόνο που θα αλλάξει στο κείμενο θα είναι οι μετατοπίσεις της κάθε στήλης μετά το χωρισμό του κειμένου σε γραμμές. Επομένως το μόνο που προκαλεί ο αλγόριθμος του Καίσαρα είναι μετατόπιση της κατανομής των γραμμάτων και ο δείκτης σύμπτωσης δεν επηρεάζεται από τέτοιες μετατοπίσεις.

Από τη στιγμή που η Eve καταφέρει και ανακτήσει κάποιο κλειδί μετά δεν χρειάζεται να επαναληφθεί η ίδια διαδικασία. Έχοντας ένα κλειδί, η Eve μπορεί να δοκιμάσει τις 26 δυνατές αποκρυπτογραφήσεις του Vigenere που προκύπτουν

από τα 26 δυνατά shift του Vigenere και να κρατήσει το κλειδί που αντιστοιχεί στην κατανομή των συχνοτήτων των γραμμάτων που προσεγγίζει περισσότερο την κατανομή των συχνοτήτων των γραμμάτων στην αγγλική γλώσσα.

2.

Χρησιμοποιώντας το κλειδί cryptography και αποκρυπτογραφώντας σύμφωνα με το Vigenere προκύπτει ένα κείμενο όμοιο με το αρχικό, κρυπτογραφημένο με τον αλγόριθμο του Καίσαρα, οπότε δοκιμάζουμε όλες τις διαφορετικές μετατοπίσεις και κρατάμε τη μετατόπιση που αντιστοιχεί στην κατανομή των συχνοτήτων εμφάνισης των γραμμάτων σε ένα κείμενο της αγγλικής γλώσσας. Έτσι αν $\vec{r}$ οι συχνότητες εμφάνισης των γραμμάτων σε ένα κείμενο της αγγλικής γλώσσας και $\vec{x_i}$ οι συχνότητες εμφάνισης των γραμμάτων στο αποκρυπτογραφημένο με Vigenere κείμενο μετατοπισμένο κατά i τότε, επιλέγουμε τη μετατόπιση

$$\min_i \{distance(\vec{r}, \vec{x_i})\}$$

Εδώ χρησιμοποιήθηκε η ευκλείδεια απόσταση.

Το αρχικό κλειδί ήταν: gvctxskvetlc.

Το plaintext ήταν:

Hi Bob. I think we have finally managed to win Eve, but we should think of a better way to encrypt our messages. I still want to use the Vigenere cipher. Can you think of a way to make our messages impossible to decrypt for her?

Ο κώδικας επισυνάπτεται.

3.

Ο Vigenere δεν μπορεί να έχει τέλεια μυστικότητα εκτος αν χρησιμοποιείται τυχαίο κλειδί με μήκος ίσο με το αρχικό κείμενο. Όμως σε αυτή την περίπτωση είναι ίδιος με το one-time pad. Έτσι η απάντηση του Bob στην Alice φαίνεται παρακάτω:

Hi Alice! We can't achieve perfect secracy using the vigenere cipher unless the key is as long as the plaintext. Then the vigenere cipher becomes the same as the one-time-pad.

Η κρυπτογραφημένη απάντηση είναι:

Qg Fhixr! Ul yos'c yhdizic wafknay oexeyju ixrll phz ignabjac hepcrp bjzjbq yde frw po ox umsc an gfl lzfrlyaxo. Gflj hmn tnceirpl ywuqcw xexbklo hmn qfie vf roa csn-rnie-knb.

Το κρυπτογραφημένο κείμενο δεν είναι πάντα το ίδιο αφού το shift επιλέγεται τυχαία. Ο κώδικας επισυνάπτεται.

Άσκηση 2

Η μέθοδος που χρησιμοποιήθηκε είναι ίδια με αυτή που περιγράφηκε προηγούμενως. Αρχικά πρέπει να προσδιοριστεί το μήκος του κλειδιού που χρησιμοποιήθηκε. Έτσι υποθέτουμε μήκος κλειδιού l και χωρίζουμε το ciphertext σε l στήλες. Στη συνέχεια υπολογίζουμε το δείκτη σύμπτωσης της κάθε στήλης όπως αυτός ορίστηκε παραπάνω και υπολογίζουμε το μέσο δείκτη σύμπτωσης όλων των στηλών. Τελικά το σωστό μήκος κλειδιού είναι αυτό που αντιστοιχεί στο μεγαλύτερο μέσο δείκτη σύμπτωσης. Έχοντας βρει μήκος κλειδιού l χωρίζουμε το κείμενο σε l στήλες και προσπαθούμε να κατασκευάσουμε ένα κείμενο που είναι ίδιο με το plaintext αλλά ολισθημένο κατά κάποιο αριθμό θέσεων. Για το σκοπό αυτό χρησιμοποιούμε το δείκτη αμοιβαίας σύμπτωσης. Πρώτα υπολογίζουμε την στήλη i η οποία αντιστοιχεί σε μέγιστο δείκτη σύμπτωσης. Ύστερα υπολογίζουμε το δείκτη αμοιβαίας σύμπτωσης κάθε στήλης j με τη στήλη i για κάθε δυνατή ολίσθηση της στήλης j και κρατάμε τη μετατόπιση που αντιστοιχεί στο μεγαλύτερο δείκτη αμοιβαίας σύμπτωσης. Έχοντας βρει πλέον μία ολίσθηση του κλειδιού δοκιμάζουμε όλες τις δυνατές ολισθήσεις και κρατάμε εκείνη για την οποία η κατανομή των συχνοτήτων εμφάνισης των γραμμάτων προσεγγίζει περισσότερο εκείνη της αγγλικής γλώσσας.

Το κλειδί που χρησιμοποιήθηκε είναι: khalilgib

Το plaintext είναι: AND A WOMAN WHO HELD A BABE AGAINST HER BOSOM SAID SPEAK TO US OF CHILDREN AND HE SAID YOUR CHILDREN ARE NOT YOUR CHILDREN THEY ARE THE SONS AND DAUGHTERS OF LIFES LONGING FOR ITSELF THEY COME THROUGH YOU BUT NOT FROM YOU AND THOUGH THEY ARE WITH YOU YET THEY BELONG NOT TO YOU YOU MAY GIVE THEM YOUR LOVE BUT NOT YOUR THOUGHTS FOR THEY HAVE THEIR OWN THOUGHTS YOU MAY HOUSE THEIR BODIES BUT NOT THEIR SOULS FOR THEIR SOULS DWELL IN THE HOUSE OF TOMORROW WHICH YOU CANNOT VISIT NOT EVEN IN YOUR DREAMS YOU MAY STRIVE TO BE LIKE THEM BUT SEEK NOT TO MAKE THEM LIKE YOU FOR LIFE GOES NOT BACKWARD NOR TARRIES WITH YESTERDAY YOU ARE THE BOWS FROM WHICH YOUR CHILDREN AS LIVING ARROWS ARE SENT FORTH THE ARCHER SEES THE MARK UPON THE PATH OF THE INFINITE AND HE BENDS YOU WITH HIS MIGHT THAT HIS ARROWS MAY GO SWIFT AND FAR LET YOUR BENDING IN THE ARCHERS HAND BE FOR GLADNESS FOR EVEN AS HE LOVES THE ARROW THAT FLIES SO HE LOVES ALSO THE BOW THAT IS STABLE

Ο κώδικας επισυνάπτεται.

Άσκηση 3

1.

Η ιδέα τους δεν είναι καλή. Για μικρά κείμενα, το επαυξημένο κλειδί καθιστά την αποκρυπτογράφηση δυσκολότερη σε σχέση με τον απλό Vigenere. Στην πραγματικότητα όμως το κρυπτοσύστημα παραμένει ευάλωτο σε επιθέσεις αφού για ένα επαρκώς μεγάλο κείμενο η αποκρυπτογράφηση μπορεί να γίνει ακόμα και αν ο επιτιθέμενος δεν γνωρίζει την παραλλαγή του Vigenere που χρησιμοποιήθηκε, χρησιμοποιώντας την αποκρυπτογράφηση του απλού Vigenere. Αν ο επιτιθέμενος γνωρίζει και τη συγκεκριμένη παραλλαγή τότε μπορεί να αποκρυπτογραφήσει το κείμενο πολύ εύκολα προσδιορίζοντας και το k εκτός από το μήκος του κλειδιού. Η επίθεση στηρίζεται στο γεγονός ότι τα κλειδιά είναι εξαρτημένα μεταξύ τους αφού το κάθε ένα είναι απλώς μία ολίσθηση του προηγούμενου κατά μία σταθερά. Οι ασφαλείς τιμές του k στηρίζονται στο γεγονός ότι ο επιτιθέμενος δεν γνωρίζει ακριβώς τον αλγόριθμο που χρησιμοποιήθηκε και αποκρυπτογραφεί με βάση τον απλό Vigenere. Συνεπώς πρέπει να μεγιστοποιηθεί ο αριθμός των στηλών στις οποίες πρέπει να χωριστεί το κείμενο ώστε σε κάθε στήλη να έχουμε αλγόριθμο Καίσαρα. Για κάθε τιμή του k παράγονται $\frac{26}{gcd(k,26)}$ κρυπτοκείμενα τα οποία είναι διαφορετικά ανά 2. Συνεπώς δεν είναι όλες οι επιλογές του k το ίδιο καλές. Διακρίνουμε τις παρακάτω περιπτώσεις:

- $k = 13$: Παράγονται $\frac{26}{gcd(13,26)} = \frac{26}{13} = 2$ διαφορετικά κλειδιά
- $k = \{2n | 1 \leq n \leq 12\}$: Παράγονται $\frac{26}{2} = 13$ διαφορετικά κλειδιά
- $k = \{2n + 1 | 0 \leq n \leq 12 \wedge n \neq 6\}$: Παράγονται $\frac{26}{1} = 26$ διαφορετικά κλειδιά

Συνεπώς η καλύτερη επιλογή για το k είναι κάποιος περιττός αριθμός εκτός απο το 13, ώστε να δημιουργηθούν 26 διαφορετικά κλειδιά.

2.

Η επίθεση βασίζεται στο γεγονός πως το κλειδί της κάθε περιόδου δεν είναι ανεξάρτητο από τα προηγούμενά του, αλλά συνδέονται μέσω μιας σχέσης ολίσθησης. Αρχικά υποθέτουμε μήκος κλειδιού n και χωρίζουμε το κρυπτοκείμενο σε γραμμές μήκους n. Στη συνέχεια υποθέτουμε κάποια τιμή του k. Η μορφή που έχουμε φέρει το κρυπτοκείμενο έχει την ιδιότητα πως αν τα n,k που υποθέσαμε είναι τα σωστά, τότε η i-οστή γραμμή είναι μετατοπισμένη κατά ik mod 26. Έτσι τροποποιούμε το κρυπτοκείμενο ως εξής:

$$\forall i. \forall j. C[i][j] \leftarrow (C[i][j] - ik) mod 26$$

όπου C[i][j] το γράμμα που βρίσκεται στη γραμμή i και στη στήλη j. Στη συνέχεια υπολογίζουμε το δείκτη σύμπτωσης κάθε στήλης ακριβώς όπως στις προηγούμενες ασκήσεις. Επαναλαμβάνοντας αυτή τη διαδικασία nk φορές για όλους τους συνδυασμούς των n και k, βρίσκουμε το ζευγάρι (n,k) που αντιστοιχεί στο μεγαλύτερο δείκτη σύμπτωσης και συνεχίζουμε την αποκρυπτογράφηση όπως στον απλό Vigenere. Έτσι δεδομένου πως οι χρήστες επιλέγουν μία απο τις ασφαλέστερες τιμές του k ο τροποποιημένος Vigenere μπορεί να σπάσει με 26 φορές περισσότερους ελέγχους.

Άσκηση 4

Έστω γλώσσα L και κείμενο μήκους N χαρακτήρων, κρυπτογραφημένο με τον αλγόριθμο Vigenere με κλειδί μήκους k. Χωρίζουμε το κείμενο σε γραμμές μήκους k. Κάθε στήλη που δημιουργείται έχει μήκος $\frac{N}{k}$ και επιπλέον όλοι οι χαρακτήρες έχουν ολισθήσει με τον ίδιο τρόπο. Θα υπολογίσουμε τη μέση τιμή του δείκτη σύμπτωσης του κρυπτοκειμένου. Επιλέγουμε 2 τυχαίους χαρακτήρες x_0, x_1 από το κρυπτοκείμενο. Θα υπολογίσουμε την πιθανότητα $Pr[x_0 = x_1]$.Διακρίνουμε τις περιπτώσεις τα x_0, x_1 να ανήκουν στην ίδια στήλη και την πιθανότητα να ανήκουν σε διαφορετικές στήλες Συμβολίζοντας με C_x τη στήλη στην οποία ανήκει το στοιχείο x:

$$\begin{aligned} Pr[x_0 = x_1] = Pr[x_0 = x_1 | C_{x_0} = C_{x_1}] Pr[C_{x_0} = C_{x_1}] + \\ + Pr[x_0 = x_1 | C_{x_0} \neq C_{x_1}] Pr[C_{x_0} \neq C_{x_1}] \end{aligned}$$

Η πιθανότητα τα x_0, x_1 να ανήκουν στην ίδια στήλη είναι:

$$Pr[C_{x_0} = C_{x_1}] = \frac{\frac{N}{k} - 1}{N - 1}$$

. Όμως όλα τα γράμματα μίας στήλης είναι ολισθημένα κατά τον ίδιο αριθμό θέσεων, οπότε ο δείκτης σύμπτωσης της κάθε στήλης προσεγγίζει τον δείκτη σύμπτωσης της γλώσσας L. Άρα έχουμε πως η πιθανότητα να επιλέξουμε 2 φορές το ίδιο γράμμα από την ίδια στήλη είναι:

$$Pr[x_0 = x_1 | C_{x_0} = C_{x_1}] = E[I_L]$$

Η πιθανότητα τα x_0, x_1 να ανήκουν σε διαφορετικές στήλες είναι:

$$Pr[C_{x_0} \neq C_{x_1}] = \frac{N - \frac{N}{k}}{N - 1}$$

Αφού όμως διαφορετικές διαφορετικές στήλες έχουν διαφορετικές ολισθήσεις τότε ο δείκτης αμοιβαίας σύμπτωσης μεταξύ τους προσεγγίζει τον δείκτη σύμπτωσης ενός τυχαίου κείμενου, όπου οι χαρακτήρες ακολουθούν ομοιόμορφη κατανομή. Άρα η πιθανότητα να επιλέξουμε 2 τυχαία στοιχεία και του κειμένου και να ταυτίζονται ενώ ανήκουν σε διαφορετικές στήλες είναι:

$$Pr[x_0 = x_1 | C_{x_0} \neq C_{x_1}] = E[I_r]$$

Τελικά, για το δείκτη σύμπτωσης του κρυπτογραφημένου κειμένου έχουμε:

$$E[I_{C_k}] = Pr[x_0 = x_1] = \frac{\frac{N}{k} - 1}{N - 1} E[I_L] + \frac{N - \frac{N}{k}}{N - 1} E[I_r]$$

$$(N-1)E[I_{C_k}] = (\frac{N}{k} - 1)E[I_L] + (N - \frac{N}{k})E[I_r]$$

$$(N-1)E[I_{C_k}] = \frac{N}{k}E[I_L] - E[I_L] + NE[I_r] - \frac{N}{k}E[I_r]$$

$$(N-1)E[I_{C_k}] + E[I_L] - NE[I_r] = \frac{N}{k}(E[I_L] - E[I_r])$$

$$k = \frac{N(E[I_L] - E[I_r])}{(N-1)E[I_{C_k}] + E[I_L] - NE[I_r]}$$

$$k = \frac{E[I_L] - E[I_r]}{\frac{N-1}{N}E[I_{C_k}] + \frac{E[I_L]}{N} - E[I_r]}$$

Επίσης:

$$\lim_{N \to \infty} \frac{E[I_L] - E[I_r]}{\frac{N-1}{N}E[I_{C_k}] + \frac{E[I_L]}{N} - E[I_r]} = \frac{E[I_L] - E[I_r]}{E[I_{C_k}] - E[I_r]}$$

Επομένως το αναμενόμενο μήκος του κλειδιού για ένα επαρκώς μεγάλο κείμενο είναι:

$$k = \frac{E[I_L] - E[I_r]}{E[I_{C_k}] - E[I_r]}$$

και άρα ισχύει η σχέση:

$$E[I_{C_k}] - E[I_r] = \frac{1}{k}(E[I_L] - E[I_r])$$

Η τιμή του $E[I_r]$ για ένα κείμενο t χαρακτήρων είναι:

$$E[I_r] = \sum_{i=1}^{t} (\frac{1}{t})^2$$

Άσκηση 5

1.

Δεν είναι αναγκαίο σε κάθε κρυπτοσύστημα που διαθέτει τέλεια μυστικότητα κάθε κλειδί να επιλέγεται με την ίδια πιθανότητα. Είναι αναγκαίο μόνο στην περίπτωση που ισχύει $|M| = |C| = |K|$. Θα το αποδείξουμε με κάποιο αντιπαράδειγμα όπου $|K| > |M|$. Συγκεκριμένα $M = \{m_0, m_1\}$, $K = \{k_0, k_1, k_2, k_3\}$ και $C = \{c_0, c_1\}$. Για το κρυπτοσύστημα αυτό ισχύει ότι:

	k_0	k_1	k_2	k_3
m_0	c_0	c_1	c_0	c_1
m_1	c_1	c_0	c_1	c_0

Επιπλέον έχουμε ότι:
$Pr[K = k_0] = Pr[K = k_1] = \frac{1}{2}$ και $Pr[K = k_2] = Pr[K = k_3] = 0$
Θα υπολογίσουμε την πιθανότητα $Pr[M = m_0|C = c_0]$:

$$Pr[M = m_0|C = c_0] = \frac{Pr[C = c_0|M = m_0]Pr[M = m_0]}{Pr[C = c_0]}$$

Έχουμε ότι:

$$Pr[C = c_0|M = m_0] = Pr[Enc_K(m_0) = c_0] = \sum_{i=0}^{3} 1_{Enc_{k_i}(m_0)=c_0} Pr[K = k_i] =$$
$$= Pr[K = k_0] + Pr[K = k_2] = \frac{1}{2} + 0 = \frac{1}{2}$$

$$Pr[C = c_0] = Pr[C = c_0|M = m_0]Pr[M = m_0] + Pr[C = c_0|M = m_1]Pr[M = m_1]$$

Ακριβώς όπως παραπάνω προκύπτει πως:

$$Pr[C = c_0|M = m_0] = Pr[C = c_0|M = m_1] = \frac{1}{2}$$

Τελικά:

$$Pr[M = m_0|C = c_0] = \frac{\frac{1}{2}Pr[M = m_0]}{\frac{1}{2}(Pr[M = m_0] + Pr[M = m_1])} = Pr[M = m_0]$$

Αντίστοιχα μπορούμε να δείξουμε ότι
$\forall m \in \{m_0, m_1\} \forall c \in \{c_0, c_1\} Pr[M = m|C = c] = Pr[M = m]$
Οπότε αν και δεν επιλέγονται όλα τα κλειδιά με την ίδια πιθανότητα, το κρυπτοσύστημα διαθέτει τέλεια μυστικότητα.

2.

i.

Ευθύ:
Έστω ότι το κρυπτοσύστημα διαθέτει τέλεια μυστικότητα.

$$Pr[C = y|M = x] = \frac{Pr[M = x|C = y]Pr[C = y]}{Pr(M = x)} = \frac{Pr[M = x]Pr[C = y]}{Pr(M = x)} = Pr[C = y]$$

όπου η δεύτερη ισότητα προκύπτει από το γεγονός πως το κρυπτοσύστημα διαθέτει τέλεια μυστικότητα.

Αντίστοφο:
Έστω ότι ισχύει $Pr[C = y|M = x] = Pr[C = y]$

$$Pr[M = x|C = y] = \frac{Pr[C = y|M = x]Pr[M = x]}{Pr[C = y]} = \frac{Pr[C = y]Pr[M = x]}{Pr[C = y]} = Pr[M = x]$$

ii.

Ευθύ:
Έστω ότι το κρυπτοσύστημα διαθέτει τέλεια μυστικότητα. Από την προηγούμενη ισοδύναμη συνθήκη έχουμε πως

$$\forall x \in M, y \in C : Pr[C = y|M = x] = Pr[C = y]$$

Συνεπώς:

$$\forall x_1, x_2 \in M, y \in C : Pr[C = y|M = x_1] = Pr[C = y|M = x_2] = Pr[C = y]$$

Αντίστροφο:
Έστω ότι ισχύει $\forall x_1, x_2 \in M, y \in C : Pr[C = y|M = x_1] = Pr[C = y|M = x_2]$
Τότε $Pr[C = y|M = x] = c$ (σταθερό). Έτσι έχουμε:

$$Pr[M = m|C = y] = \frac{Pr[C = y|M = x]Pr[M = x]}{Pr[C = y]} =$$
$$= \frac{Pr[C = y|M = x]Pr[M = x]}{\sum_{x' \in M} Pr[C = y|M = x']Pr[M = x']} =$$
$$= \frac{cPr[M = x]}{\sum_{x' \in M} cPr[M = x']} = \frac{cPr[M = x]}{c\sum_{x' \in M} Pr[M = x']} = Pr[M = x]$$

Επομένως το κρυπτοσύστημα διαθέτει τέλεια μυστικότητα.

Άσκηση 6

1.

Ένα λατινικό τετράγωνο τάξης 5 φαίνεται παρακάτω:

1	2	3	4	5
5	1	2	3	4
4	5	1	2	3
3	4	5	1	2
2	3	4	5	1

α.

$Enc_1(3) = l_{1,3} = 3$
$Enc_2(3) = l_{2,3} = 2$
$Enc_3(3) = l_{3,3} = 1$
$Enc_4(3) = l_{4,3} = 5$
$Enc_5(3) = l_{5,3} = 4$

β.

$Enc_4(1) = l_{4,1} = 3$
$Enc_4(2) = l_{4,2} = 4$
$Enc_4(3) = l_{4,3} = 5$
$Enc_4(4) = l_{4,4} = 1$
$Enc_4(5) = l_{4,5} = 2$

2.

Θα αποδείξουμε ότι το κρυπτοσύστημα έχει τέλεια μυστικότητα:

$$Pr[M = x|C = y] = \frac{Pr[C = y|M = x]Pr[M = x]}{Pr[C = y]}$$

Όμως:

$$\forall x \in M, y \in C : Pr[C = y|M = x] = Pr[Enc_K(M) = y|M = x] = Pr[Enc_K(x) = y] =$$
$$= \sum_{k=1}^{n} 1_{Enc_k(x)=y} Pr[K = k] = \sum_{k=1}^{n} 1_{l(k,x)=y} Pr[K = k] = \frac{1}{|K|} = \frac{1}{n}$$

όπου οι τελευταίες ισότητες ισχύουν λόγω της κατασκευής του πίνακα (μοναδική εμφάνιση κάθε ciphertext σε κάθε γραμμή και στήλη) αφού για κάθε ζεύγος $x \in M, y \in C$ υπάρχει μοναδικό $k \in K$ τέτοιο ώστε $Enc_k(x) = y$.

Συνεπώς:

$$\frac{Pr[C = y|M = x]Pr[M = x]}{Pr[C = y]} = \frac{\frac{1}{n}Pr[M = x]}{\sum_{x' \in M} Pr[C = y|M = x']Pr[M = x']}$$
$$= \frac{\frac{1}{n}Pr[M = x]}{\frac{1}{n}\sum_{x' \in M} Pr[M = x']} = Pr[M = x]$$

Άρα $Pr[M = x|C = y] = Pr[M = x]$ και το κρυπτοσύστημα διαθέτει τέλεια μυστικότητα.