ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΚΡΥΠΤΟΓΡΑΦΙΑ

(2021 – 2022)

1η Σειρά Ασκήσεων

Ονοματεπώνυμο:

- Χρήστος Τσούφης

Αριθμός Μητρώου:

- 031 17 176

Στοιχεία Επικοινωνίας:

- el17176@mail.ntua.gr
- chris99ts@gmail.com

1η Άσκηση

Η Alice θέλει να επικοινωνήσει με τον φίλο της τον Bob κρυφά, αλλά η κακόβουλη Eve θέλει να υποκλέψει την συνομιλία τους και να μάθει τα σχέδια τους. Η Alice με τον Bob ξέρουν ότι κάτι σχεδιάζει η Eve και γι' αυτό αποφασίζουν να κρυπτογραφούν τα μηνύματα τους με το κρυπτοσύστημα Vigenère. Μετά από μερικά μηνύματα αντιλαμβάνονται ότι η Eve είναι αρκετά έξυπνη και έχει με κάποιο τρόπο βρει το κλειδί που χρησιμοποίησαν. Έτσι, αποφασίζουν να κρυπτογραφούν και τα κλειδιά τους έτσι ώστε η Eve να μην μπορεί να τα βρει. Για το σκοπό αυτό χρησιμοποιούν το σύστημα του Καίσαρα για να τροποποιήσουν τα κλειδιά τα οποία στη συνέχεια χρησιμοποιούν για κρυπτογράφηση με το σύστημα Vigenère.

1. *Με ποια τεχνική θεωρείτε ότι η Eve κατάφερε αρχικά να αποκρυπτογραφήσει χωρίς να έχει πρόσβαση στα αρχικά κλειδιά, αλλά ξέροντας μόνο τα κρυπτοκείμενα; Μπορεί τώρα η Eve να χρησιμοποιήσει την ίδια τεχνική για να αποκρυπτογραφήσει τα μηνύματα παρά την τροποποίηση των κλειδιών; Πέτυχαν κάτι η Alice και ο Bob με την τροποποίηση των κλειδιών με το σύστημα του Καίσαρα; Εξηγήστε.*

2. *Μπείτε στην θέση της Eve και θέλετε να αποκρυπτογραφήσετε τα μηνύματα. Ξέρετε ότι το αρχικό κλειδί πριν την τροποποίηση με Καίσαρα είναι* ***cryptography****. Ξέρετε ακόμη ότι τελικό κρυπτοκείμενο είναι αυτό:*

```
Nd Dhy. A dcmgv yk ccob xsieewa svptdwn os ptp Kqg, url gz wazwry vaffu jj
t mgzogk tsi os xyextrm lmb hildcmzu. B plsgp plpz oq npw dci Otikigkb
usklxc. Egi ahr lrdrd zh g rcr qg wvox zwx hglpsqzw bxrunubydo os wpextrm
cgb cik?
```

Γράψτε κώδικα σε Python, C, C++, Java, ή Haskell που θα σας βοηθήσει να σπάσετε τον κρυπτοκείμενο. Ποιο είναι το αρχικό κείμενο, και ποιο το κλειδί που χρησιμοποιήθηκε στο σύστημα του Καίσαρα; Δείξτε τον κώδικα που αναπτύξατε (άλλοι τρόποι λύσης γίνονται δεκτοί, ενδεχομένως με μειωμένη βαθμολογία, εφόσον τους αναφέρετε).

3. *Παραπάνω η Alice έκανε μια ερώτηση. Τώρα είστε ο Bob. Απαντήστε στην ερώτηση της! Μετά γράψτε κώδικα που θα κρυπτογραφεί την απάντηση με το ίδιο σύστημα που χρησιμοποίησε η Alice πριν και δείξτε την κρυπτογραφημένη απάντηση. Επίσης, δείξτε τον κώδικα που αναπτύξατε (άλλοι τρόποι λύσης γίνονται δεκτοί, ενδεχομένως με μειωμένη βαθμολογία, εφόσον τους αναφέρετε).*

Λύση:

1. Η επίλυση αυτού του ερωτήματος αναπτύσσεται σε αναλυτικά με 2 τρόπους που ίσως να έχουν κάποιες επικαλύψεις αλλά έγινε ο διαχωρισμός τους για να αναδειχθεί καλύτερα ο τρόπος προσέγγισης της κάθε επίλυσης.

1ος Τρόπος Επίλυσης:

Η Eve χρησιμοποιώντας μια από τις γνωστές μεθόδους κρυπτανάλυσης του Vigenere, κατάφερε να αποκρυπτογραφήσει τα μηνύματα της Alice και του Bob χωρίς να έχει πρόσβαση στα κλειδιά που χρησιμοποίησαν, γνωρίζοντας μόνο τα κρυπτοκείμενα.

Αρχικά, υπολογίζεται το μήκος του κλειδιού και έπειτα η ολίσθηση κάθε γράμματος του κλειδιού.

Το μήκος του κλειδιού μπορεί να βρεθεί με την μέθοδο του Kasiski's test ψάχνοντας κοινές συμβολοσειρές και υποθέτοντας ότι αυτές αντιστοιχούν σε κοινές συμβολοσειρές στο αρχικό κείμενο που έχουν κρυπτογραφηθεί με τον ίδιο τρόπο. Τότε, το μήκος του κλειδιού θα είναι ακέραιο πολλαπλάσιο της απόστασης των δύο συμβολοσειρών. Συνεπώς, αν βρεθούν αρκετά ζευγάρια, τότε οι κοινοί διαιρέτες των αποστάσεών τους θα δώσουν τελικά τα πιθανά μήκη κλειδιών. Εναλλακτικά, το μήκος του κλειδιού μπορεί να βρεθεί και με την χρήση δεικτών σύμπτωσης (IC), δηλαδή με την πιθανότητα δύο τυχαία επιλεγμένα γράμματα να είναι ίδια. Ειδικότερα, γίνεται ο υπολογισμός των δεικτών σύμπτωσης για διάφορα μήκη κλειδιών κατά στήλες που έχουν κρυπτογραφηθεί με τον ίδιο τρόπο και όχι σε ολόκληρο το κείμενο. Έτσι, όταν οι δείκτες σύμπτωσης σε όλες τις στήλες είναι κοντά στο δείκτη σύμπτωσης της αγγλικής γλώσσας, δηλαδή περίπου 0.065 τότε θα έχει βρεθεί το μήκος του κλειδιού.

Όσον αφορά την εύρεση της ολίσθησης, αυτή μπορεί να γίνει είτε με δοκιμές όλων των πιθανών ολισθήσεων σε κάθε στήλη μέχρι να βρεθεί εκείνη που επιτυγχάνει το μέγιστο δείκτη αμοιβαίας σύμπτωσης με ένα αγγλικό κείμενο είτε με τον υπολογισμό του δείκτη αμοιβαίας σύμπτωσης μεταξύ των στηλών με δοκιμές όλων των πιθανών ολισθήσεων έτσι ώστε όλες ανά δύο να δίνουν τον δείκτη σύμπτωσης της αγγλικής γλώσσας.

Συμπερασματικά, δεν απαιτείται η εύρεση του κλειδιού ως λέξη αλλά απλώς ως ολίσθηση των γραμμάτων. Συνεπώς, η Alice και ο Bob δεν κέρδισαν κάτι κρυπτογραφώντας το κλειδί με την μέθοδο του Καίσαρα εφόσον η Eve θα κάνει ακριβώς ότι έκανε και πριν για να πάρει τα αρχικά κείμενα.

2ος Τρόπος Επίλυσης:

Για να αποκρυπτογραφήσει η Eve τα κρυπτοκείμενα μπορεί να χρησιμοποιήσει δείκτες σύμπτωσης (IC). Αναλυτικότερα, όσο πιο πολλά κρυπτοκείμενα συλλέξει η Eve, τόσο ευκολότερη γίνεται η αποκρυπτογράφηση εφόσον το κλειδί μεταξύ τους δεν αλλάζει. Έτσι, ακολουθώντας την σειρά βημάτων που θα περιγραφεί στην συνέχεια, μπορεί να μαζέψει όλα τα κείμενα και τελικά να αποκρυπτογραφήσει το κρυπτοκείμενο. Πρώτον, θα πρέπει να χωρίσει το κρυπτοκείμενο σε m στήλες για διάφορα m μέχρι ένα σχετικά μεγάλο αριθμό, λ.χ. το 12, και να υπολογίσει το IC για κάθε στήλη για κάθε m. Έπειτα, βρίσκοντας τον μέσο όρο του IC για κάθε m μπορεί να υπολογίσει κάποια πιθανά μήκη κλειδιού. Στην συνέχεια, χρησιμοποιώντας αυτά τα πιθανά μήκη κλειδιού που υπολόγισε, θα δοκιμάσει να βρει την σχετική μετατόπιση μεταξύ της πρώτης στήλης και κάθε άλλης στήλης. Αυτό μπορεί να γίνει υπολογίζοντας τον δείκτη αμοιβαίας σύμπτωσης μεταξύ αυτών των δύο στηλών για κάθε μετατόπιση και τελικά να βρει την σχετική μετατόπιση μεταξύ της πρώτης και κάθε άλλης στήλης. Ύστερα, αρκεί να κάνει δοκιμές ώστε να αποκρυπτογραφήσει ένα μονοαλφαβητικό σύστημα Καίσαρα. Έτσι, για διάφορες μετατοπίσεις όλου του κειμένου, θα κάνει δοκιμές ώστε να βρει αυτήν που έχει δείκτη σύμπτωσης πιο κοντά στο αγγλικό κείμενο. Τελικά, όταν θα βρει τον IC τότε θα ξέρει την μετατόπιση για κάθε γράμμα και τελικά θα μπορεί να υπολογίσει το κλειδί και το plaintext.

Με αυτόν τον τρόπο, δεν είναι απαραίτητη η γνώση των κλειδιών για την αποκρυπτογράφηση του κρυπτοκειμένου. Έτσι, με την προϋπόθεση ότι ο Bob και η Alice θα συνεχίσουν να χρησιμοποιούν τα ίδια κλειδιά και ότι απλά θα τα κρυπτογραφήσουν με Καίσαρα, τότε η Eve αρκεί είτε να γνωρίζει ήδη το κλειδί, οπότε να δοκιμάσει για κάθε μετατόπιση να αποκρυπτογραφήσει το κρυπτοκείμενο και τελικά το plaintext με τον IC πιο κοντά στην τιμή για την Αγγλική γλώσσα (δηλ. 0.065) να είναι το σωστό, είτε να μην γνωρίζει το κλειδί και να ακολουθήσει την παραπάνω διαδικασία που περιγράφηκε.

Εν κατακλείδι, σε κάθε περίπτωση, ο Bob και η Alice δεν κατάφεραν να πετύχουν μεγάλη ασφάλεια, αφού, όπως αναφέρθηκε, αν η Eve γνωρίζει ήδη το κλειδί, τότε θα υπάρχουν 26 μετατοπίσεις που χρειάζεται να δοκιμάσει για να αποκρυπτογραφήσει το κείμενο (μια για κάθε πιθανή μετατόπιση της μεθόδου του Καίσαρα). Από την άλλη, αν η Eve δεν γνωρίζει το κλειδί, τότε θα ακολουθήσει τα βήματα που αναλύθηκαν ανωτέρω και τελικά θα χρειαστεί να συλλέξει ένα μεγάλο πλήθος χαρακτήρων για να μπορέσει τελικά να αποκρυπτογραφήσει το κείμενο.

2. Υπό το πρίσμα της Eve, για την αποκρυπτογράφηση του κρυπτοκειμένου, το μόνο που απαιτείται είναι να γίνουν δοκιμές όλων των δυνατών μετατοπίσεων του κλειδιού με το σύστημα του Καίσαρα και για κάθε μια να γίνει δοκιμή του αποτελέσματος αποκρυπτογράφησης που δημιουργεί. Ο ευκολότερος τρόπος για να γίνει αυτό είναι να εξεταστεί κάθε μια από τις 26 μετατοπίσεις για να βρεθεί ποιο κείμενο βγάζει νόημα στην Αγγλική γλώσσα. Το τελικό αποτέλεσμα του προγράμματος είναι το πιο πιθανό plaintext μαζί με το κλειδί και την μετατόπισή του. Έτσι προκύπτουν τα εξής:

Το plaintext είναι το ακόλουθο που προέκυψε με το κλειδί "`gvctxskvetlc`" και με shifting:

"`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 python που υλοποιεί το παραπάνω ερώτημα επισυνάπτεται στο zip αρχείο που υποβλήθηκε.

3. Για την βελτίωση της ασφάλειας της επικοινωνίας μεταξύ Bob και Alice θα ήταν εφικτή εάν χρησιμοποιηθεί κλειδί μιας χρήσης με μήκος όσο το κείμενο που στέλνεται κάθε φορά. Αυτή η μέθοδος μοιάζει με την One Time Pad και τότε είναι αδύνατο να αποκρυπτογραφηθεί το κείμενο αφού όσο χρησιμοποιείται το ίδιο κλειδί για την ανταλλαγή μηνυμάτων, η Eve μπορεί να συλλέγει τα κρυπτοκείμενα και τελικά να κάνει την κρυπτανάλυση που εξηγήθηκε και να βρει το κείμενο.

Το plaintext και, για κλειδί το "`cryptography`", το ciphertext θα είναι τα ακόλουθα:

"`Hello there. We have to do something in order to outsmart Eve. However, if we must use the Vigenere cipher, we should probably use the One Time Pad method with a random big key just to be sure.`"

"`Nznel lrzvx. Hg nvxx qg nj whxgzckgd ax jvwpt zj qnqkwvvm Pxk. Cqpbnom, my hg spum rko olx Gkmzpxow mdtapt, cz ualmvy tkzdgwnr rko olx Zpk Okfb Hky qxejuy ybqz k megoqs wkz hwi eyle vu wg lrjo.`"

Ο κώδικας python που υλοποιεί το παραπάνω ερώτημα επισυνάπτεται στο zip αρχείο που υποβλήθηκε.

2η Άσκηση

Δύο φίλοι προσπαθούν να αυξήσουν την ασφάλεια του κρυπτοσυστήματος Vigenere. Σκέφτονται να επαυξήσουν το κλειδί με έναν ακέραιο αριθμό k, και σε κάθε νέα περίοδο να χρησιμοποιούν ένα νέο κλειδί, που προκύπτει ολισθαίνοντας το προηγούμενο κλειδί κατά k.

***(α)** Είναι καλή η ιδέα; Επιχειρηματολογήστε. Υπάρχουν καλύτερες και χειρότερες επιλογές για το k;*

***(β)** Προτείνετε μια όσο το δυνατόν πιο αποδοτική επίθεση στο σύστημα αυτό, υποθέτοντας ότι γνωρίζετε την μέθοδο που ακολουθούν και ότι αγνοείτε μόνο το επαυξημένο κλειδί, δηλ. την κωδική λέξη και το k.*

Λύση:

(α) *1ος Τρόπος Επίλυσης*:

Η ιδέα φαίνεται να είναι καλή για την αύξηση της δυσκολίας επίθεσης του κρυπτοσυστήματος, δηλαδή της ασφάλειας, αφού χωρίς μεγάλες αλλαγές είναι σαν να γίνεται κρυπτογράφηση με μεγαλύτερο κλειδί με την κατάλληλη επιλογή του k. Επιπλέον, οι επιθέσεις που αναφέρθηκαν παραπάνω δεν είναι το ίδιο αποτελεσματικές. Πιο συγκεκριμένα, αυτό που πετυχαίνουν είναι ότι η στατιστική συχνότητα των γραμμάτων του κρυπτοκειμένου είναι πολύ πιο δύσκολη να βρεθεί αφού η κάθε στήλη του Vigenere τώρα δεν ανήκει στο ίδιο αλφάβητο και δεν θα έχει IC κοντά στο Αγγλικό. Επιπλέον, το σύστημα αυτό εξουδετερώνει το Kasiski test αφού πλέον θα είναι αρκετά δυσκολότερο να βρεθούν όμοιες ακολουθίες χαρακτήρων στο κείμενο.

Όσον αφορά το k, αναζητείται τέτοιο ώστε οι αρχικοί χαρακτήρες του κλειδιού να επαναλαμβάνονται όσο λιγότερο γίνεται. Επομένως, ακατάλληλες είναι οι τιμές που ανήκουν στο διάστημα [0, 13]. Αντιθέτως, οι υπόλοιπες τιμές οδηγούν σε μετατοπίσεις του αρχικού κλειδιού που θα είναι διαφορετικό για πολύ μεγάλο αριθμό περιόδων. Επιπλέον, αριθμοί μεγαλύτεροι από το μήκος του αλφαβήτου δεν συνεισφέρουν κάποια επιπλέον ασφάλεια αφού θα παραμείνει μόνο το υπόλοιπό τους με το 26 (δηλ. mod 26). Ειδικότερα, θα πρέπει ο αριθμός k να είναι σχετικά πρώτος με το 26, δηλαδή gcd(k, 26) = 1, διότι σε κάθε περίοδο γίνεται ολίσθηση του κλειδιού κατά k mod 26. Έτσι, για έναν πλήρη κύκλο για να γίνει κρυπτογράφηση με το ίδιο κλειδί θα πρέπει να περάσει από όλα τα δυνατά υπόλοιπα mod 26, που είναι 26 στο πλήθος. Αντιθέτως, η χειρότερη επιλογή είναι k mod 26 = 0, αφού τότε δεν αλλάζει ποτέ το κλειδί και έτσι το σύστημα παραμένει Vigenere. Επίσης, για k mod 26 = 13 στην 2η περίοδο θα πρέπει να γίνει ολίσθηση του κλειδιού κατά 13 θέσεις ενώ στην 3η περίοδο θα πρέπει να γίνει ολίσθηση του κλειδιού κατά 26 που αντιστοιχεί στο κλειδί της 1ης περιόδου. Σημειώνεται ότι σε κάθε άλλη περίπτωση θα χρειαστούν 13 περίοδοι για την κρυπτογράφηση με το ίδιο κλειδί οπότε παρατηρείται ότι το κλειδί επαναλαμβάνεται κάθε $^{26}/_{\gcd(k,26)}$ περιόδους και συνεπώς το σύστημα ισοδυναμεί με απλό Vigenere.

2ος Τρόπος Επίλυσης:

Αρχικά, εξετάζεται το αποτέλεσμα των διαφορετικών τιμών του k στο τελικό κλειδί. Έχει σημασία να εξεταστούν τα διαφορετικά ενδεχόμενα για τον αριθμό k mod 26 καθώς για οποιαδήποτε τιμή του k, οι κυκλικές μετατοπίσεις ανάγονται σε αυτούς τους 26 αριθμούς και τελικά αρκούν τα $k \in [0, 25]$. Ακόμα και με την ολίσθηση θα προκύπτει μια περιοδικότητα στο κλειδί, αφού για ένα γράμμα m μετά από n μετατοπίσεις, θα έχει προκύψει το γράμμα $(m+n \cdot k \bmod 26)$ και όταν το $(n \cdot k \bmod 26 = 0)$ τότε θα έχει ολοκληρωθεί μια περίοδος και τα διαδοχικά κλειδιά θα αρχίσουν να ξαναπαίρνουν τις ίδιες τιμές. Ειδικότερα, αφού το 26 σε γινόμενο πρώτων παραγόντων, αναλύεται σε $2 \cdot 13$, τότε για τα k που διαιρούνται με το 2, κάθε 13 επαναλήψεις θα προκύπτουν ξανά τα ίδια κλειδιά (δηλαδή, για k = 13, κάθε 2 επαναλήψεις θα προκύπτουν ίδια κλειδιά, για k = 0 κάθε φορά θα προκύπτει το ίδιο κλειδί και για k που είναι σχετικά πρώτα με το 26 θα προκύπτουν οι ίδιοι αριθμοί κάθε 26 επαναλήψεις). Έτσι, ακόμη και αν αγνοηθεί η πληροφορία που δίνει η σταθερή ολίσθηση του αρχικού κλειδιού, παρατηρείται ότι το πρόβλημα και πάλι ανάγεται σε Vigenere απλώς με μεγαλύτερο μήκος κλειδιού.

Πιο αναλυτικά, για k = 0, προκύπτει ο κλασσικός Vigenere cipher και για ολίσθηση 13 θέσεων δεν προστίθεται ιδιαίτερη πολυπλοκότητα στο πρόβλημα. Στις περιπτώσεις τώρα, το μήκος του κλειδιού μεγαλώνει αλλά είναι γνωστό ότι το νέο κλειδί έχει σίγουρα μήκος πολλαπλάσιο του 13 ή και του 26. Επιπλέον, αυτά τα νέα κλειδιά δεν μπορούν να πάρουν όλες τις πιθανές διαφορετικές τιμές καθώς εξαρτώνται από το αρχικό τους κλειδί οπότε δεν αυξάνεται ιδιαίτερα η πολυπλοκότητα του προβλήματος.

Συνεπώς, θα κατέληγε κανείς στο γεγονός ότι είναι καλύτερο να επιλέγονται αριθμοί πρώτοι με το 26 για το k έτσι ώστε να μεγαλώσει όσο το δυνατόν περισσότερο το νέο κλειδί, όμως τότε ελλοχεύει ο κίνδυνος της γνώσης του μήκους του νέοι κλειδιού, αφού θα είναι πολλαπλάσιο του 26. Για την περίπτωση που δεν επιλεχθούν οι τιμές k = 0, 13 τότε και πάλι θα είναι γνωστό ότι το μήκος του κλειδιού θα είναι πολλαπλάσιο του 13, αφού για k = 0, προκύπτει κλασσικός Vigenere cipher οπότε ουσιαστικά δεν αλλάζει κάτι με τις προσθήκες που έγιναν ενώ, για k = 13, θα είναι γνωστές οι μετατοπίσεις οπότε και πάλι θα μπορεί να γίνει η αναγωγή σε κλασσικό Vigenere cipher. Επομένως, δεν φαίνεται να υπάρχουν κάποιες τιμές του k που να είναι προτιμότερες από άλλες.

(β) *1ος Τρόπος Επίλυσης*:

Το παραπάνω σύστημα ίσως να μπορεί να σπάσει με κάποιες παραλλαγές της επίθεσης που περιγράφηκε στην 1η άσκηση με τους δείκτες σύμπτωσης. Αναλυτικότερα, για τα πιθανά κλειδιά αρκεί να γίνει δοκιμή επιπλέον όλων των ολισθήσεων για το k, οι οποίες λόγω του mod 26 θα είναι 26 στο πλήθος. Έπειτα, αναζητούνται οι συνδυασμοί που δίνουν δείκτη σύμπτωσης κοντά σε αυτόν της Αγγλικής γλώσσας. Τέλος, εφαρμόζεται ως έχει το Βήμα 2 για την σχετική ολίσθηση μεταξύ των γραμμάτων του κλειδιού. Με άλλα λόγια, μια αποδοτική επίθεση στο σύστημα είναι παρόμοια με μια επίθεση στο σύστημα Vigenere. Αναλυτικότερα, αρχικά το σύστημα χωρίζεται σε m στήλες για διάφορους αριθμούς m, όπου m θα είναι το μήκος του κλειδιού. Για κάθε στήλη γίνεται ολίσθηση όλων των γραμμάτων κατά k χαρακτήρες από το προηγούμενο για $k \in \{0, \ldots, 26\}$. Έτσι, είναι εφικτός ο υπολογισμός του IC για την κάθε ολίσθηση για κάθε στήλη. Επομένως, εάν έχουν βρεθεί τα σωστά m, k, το μέσο IC όλων των στηλών θα πρέπει να είναι κοντά στο IC της Αγγλικής γλώσσας. Τέλος, η επίθεση ολοκληρώνεται με παρόμοιο τρόπο με την επίθεση σε Vigenere. Από την παραπάνω επίθεση είναι φανερό ότι η χρήση της επαύξησης του Vigenere οδηγεί στον υπολογισμό $26 \cdot m$ δοκιμών, αφού για κάθε μήκος κλειδιού θα πρέπει να δοκιμασθούν 26 ολισθήσεις των γραμμάτων της στήλης.

2ος Τρόπος Επίλυσης:

Λαμβάνοντας υπόψιν τον 2ο Τρόπο Επίλυσης του ερωτήματος (α), ένας αποδοτικός αλγόριθμος για την επίλυση του προβλήματος θα μπορούσε να προκύψει με την χρήση των δεικτών σύμπτωσης. Έτσι, μπορούν να αναζητηθούν μήκη κλειδιού πολλαπλάσια του 13, αν προκύψει κλειδί με μήκος p·13, όπου p περιττός, ώστε το αρχικό κλειδί να έχει μήκος p. Ακόμη, αν προκύψουν μήκη κλειδιού με μήκος p·13, όπου τώρα p άρτιος, τότε το αρχικό κλειδί θα είχε μήκος είτε p ή 2·p. Τελικά, όταν επιλεχθεί ένα πιθανό αρχικό μήκος κλειδιού από αυτές τις περιπτώσεις που αναφέρθηκαν θα υπάρχουν 12 διαφορετικά k από τα οποία θα μπορεί να προέκυψε. Έπειτα, αφού εξεταστούν όλα αυτά τα ενδεχόμενα μπορεί να καταλήξει κανείς στο k με τους καλύτερους δείκτες σύμπτωσης. Επομένως, γνωρίζοντας το μήκος του αρχικού κλειδιού και το k, μπορεί να γίνει αναγωγή του προβλήματος σε κλασσικό Vigenere. Σημειώνεται ότι εάν δεν βρεθεί το κλειδί στα πολλαπλάσια του 13, τότε αντιμετωπίζεται σαν ένα κλασσικό Vigenere, ενώ αν δεν βρεθεί το μήκος του κλειδιού τότε σημαίνει ότι και το αρχικό κλειδί ήταν πολύ μεγάλου μήκους. Έτσι, θεωρώντας |K| το μήκος του κειμένου τότε το μήκος του αρχικού κλειδιού θα είναι:

$|K| < 1.47 \cdot 26 \cdot m$ (Unicity Distance) $\Rightarrow \frac{|K|}{38.22} < m < |K|$ (Brute Force method) $\Rightarrow \frac{|K|}{38.22} < m < \frac{|K|}{19.11}$

Έτσι, για κάθε μήκος m εξετάζονται και τα 12 k που είναι πρώτοι με το 26 και αναζητείται ένας καλός δείκτης σύμπτωσης.

Έτσι, για $\frac{|K|}{19.11} < m < \frac{|K|}{2.94}$ για όλα τα k εκτός από τις τιμές 13, 26, αναζητείται ένας καλός δείκτης σύμπτωσης και για $\frac{|K|}{2.94} < m < \frac{|K|}{1.47}$ αναζητούνται όλα τα k εκτός από το 26.

Εάν και σε αυτή την περίπτωση δεν βρεθεί καλός δείκτης σύμπτωσης που να δίνει το μήκος του κλειδιού τότε μάλλον έχει χρησιμοποιηθεί μεγαλύτερο κλειδί και τότε είναι δύσκολο να αποκρυπτογραφηθεί.

3η Άσκηση

Να αποδείξετε ότι για το κρυπτοσύστημα Vigenere ισχύει η σχέση $E[I_{C_k}] - E[I_r] = \frac{1}{k}(E[I_L] - E[I_r])$*, όπου* $E[I_{C_k}]$ *είναι η αναμενόμενη τιμή του δείκτη σύμπτωσης κρυπτοκειμένου που έχει προκύψει από κλειδί μήκους k (με όλα τα γράμματα διαφορετικά), E[L] η αναμενόμενη τιμή του δείκτη σύμπτωσης για κείμενο γλώσσας L, και E[r] η αναμενόμενη τιμή του δείκτη σύμπτωσης για εντελώς τυχαίο κείμενο με χαρακτήρες από το αλφάβητο της γλώσσας L. Ποια είναι η τιμή του E[r] αν η γλώσσα L έχει t χαρακτήρες;*

Λύση:

Υπολογισμός του όρου $E[I_{C_k}]$:

Το IC αναπαριστά την πιθανότητα δύο γράμματα του κειμένου να είναι τα ίδια. Επίσης, μπορεί να υποθέσει κανείς ότι το κείμενο διαιρείται τέλεια από το μήκος του κλειδιού. Η τιμή του $E[I_{C_k}]$ ισούται με την πιθανότητα δύο γράμματα μέσα στο κρυπτοκείμενο να είναι ίδια. Αυτό μπορεί να συμβεί είτε όταν ανήκουν στην ίδια στήλη κατά την επίθεση σε Vigenere με IC είτε όταν δεν ανήκουν. Ειδικότερα,

- Έστω ότι τα γράμματα ανήκουν στην ίδια στήλη κατά την επίλυση του Vigenere με IC και άρα ουσιαστικά είναι το ίδιο γράμμα στο αρχικό κείμενο. Έτσι, η επιλογή τους έχει γίνει με πιθανότητα $E[I_L]$. Επιπλέον, η πιθανότητα να είναι γράμματα της ίδιας στήλης είναι $\frac{\frac{n}{k}-1}{n-1}$ διότι υπάρχουν k στήλες και $\frac{n}{k}$ γράμματα σε κάθε στήλη. Έτσι, αν επιλεχθεί ένα γράμμα τότε η πιθανότητα να επιλεχθεί ένα άλλο γράμμα από την στήλη είναι ίση με το πλήθος των υπολειπόμενων γραμμάτων της στήλης δια τα συνολικά υπολειπόμενα γράμματα. Εν τέλει, η πιθανότητα είναι: $\frac{\frac{n}{k}-1}{n-1} * E[I_L]$.

- Έστω ότι τα γράμματα δεν ανήκουν στην ίδια στήλη αλλά είναι ίδια. Αυτή η περίπτωση αντιστοιχεί στην επιλογή δύο γραμμάτων από μια άλλη γλώσσα, εφόσον δεν είναι γνωστή κάποια πληροφορία για το κλειδί ή το αρχικό κείμενο που να οδηγεί σε παραπάνω συμπεράσματα, και επίσης σημειώνεται ότι τα γράμματα αυτά ανήκουν σε διαφορετικούς κώδικες Καίσαρα. Αυτή η πιθανότητα είναι η $E[I_r]$. Επιπροσθέτως, η πιθανότητα να επιλεχθούν δύο τυχαία γράμματα και αυτά να ανήκουν σε διαφορετικές στήλες είναι $\frac{n-\frac{n}{k}}{n-1}$. Αυτό ισχύει διότι, εάν επιλεχθεί ένα γράμμα από μια στήλη, τότε θα υπάρχουν $n - \frac{n}{k}$ υπολειπόμενα γράμματα που ανήκουν σε άλλες στήλες και συνολικά n – 1 υπολειπόμενα γράμματα. Εν τέλει, η πιθανότητα είναι: $\frac{n-\frac{n}{k}}{n-1} * E[I_r]$.

Επομένως, για το $E[I_{C_k}]$ είναι:

$$E[I_{C_k}] = \frac{\frac{n}{k}-1}{n-1} * E[I_L] + \frac{n-\frac{n}{k}}{n-1} * E[I_r] \quad \Rightarrow$$

$$(n-1) * E[I_{C_k}] = (\frac{n}{k} - 1) * E[I_L] + (n - \frac{n}{k}) * E[I_r] \quad \Rightarrow$$

$$(n-1) * E[I_{C_k}] + E[I_L] - n * E[I_r] = \frac{n}{k}(E[I_L] - E[I_r]) \quad \Rightarrow$$

$$n * (E[I_{C_k}] - E[I_r]) + (E[I_L] - E[I_{C_k}]) = \frac{n}{k}(E[I_L] - E[I_r]) \quad \Rightarrow$$

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

Οπότε, αν θεωρηθεί ότι το $\frac{E[I_{C_k}] - E[I_r]}{n}$ είναι μια σταθερά και άρα μια αμελητέα ποσότητα, αφού η διασπορά δύο συγκρίσιμων αριθμών διαιρείται με το n το οποίο ακόμα και για μικρές προτάσεις θα είναι πολύ μεγαλύτερο του k και τάξης μεγέθους στους εκατοντάδες χαρακτήρες, τότε τελικά θα προκύψει η ζητούμενη ισότητα.

Αν η γλώσσα L έχει t χαρακτήρες, τότε ο δείκτης σύμπτωσης ενός τυχαίου κειμένου με t χαρακτήρες δίνεται από την σχέση: $E[I_r] = \sum_{n=0}^{t} \Pr[x = t_i] * \Pr[y = t_i] = \sum_{n=0}^{t} \frac{1}{t^2} = \frac{1}{t}$

4η Άσκηση

Να γράψετε πρόγραμμα σε γλώσσα Python, C/C++, ή άλλη γλώσσα της επιλογής σας, με τις συνήθεις βιβλιοθήκες, που να δέχεται ως είσοδο κρυπτοκείμενα κρυπτογραφημένα με Vigenère και να εξάγει το πολύ 10 πιθανά plaintexts και τα αντίστοιχα κλειδιά (ένα από αυτά θα πρέπει να αντιστοιχεί ακριβώς στο σωστό, με όλα τα γράμματα σωστά). Το πρόγραμμά σας θα πρέπει να εξάγει και τον δείκτη σύμπτωσης καθενός plaintext.

Να εξηγήσετε τις βασικές ιδέες που χρησιμοποιήσατε στον κώδικά σας.

Κρυπτοκείμενο εισόδου:

```
KUDLEZSIOGOOSMWJICKIELOLOVTDOECJZYWNCHIOAAKILDVUDWQIPJVKRPVLTLIOZATLJUCSM
OIWLCKVBBLNZBJUCSMOIWLCKVURLYLZPZPFCVNDIYJLBENHEMCYWGVPFPAWUVHSUGQWCOBTOS
FEPPEKPWLTSZZAOIIVUMCETWUPYOXGZAIONAHZCRNBIOFACMHOBIIVUJMEZPFIIEWWYMVPDAO
JWFEWVWHYRQGKBIOTYZCCRWWOIUEVZZGPEYTSWFMPUCMOCBSKGIKCEEPPOZPGUTSWFMPUCFOF
ULEPPEZEEPPOZCYKIPAMABOYATSMTXAPESSQWCZPFSYSZCWYLXOSLTVENMIYBSPWQZWNYYRZE
HNQDRFOFKLTVPDCIDQETWUOCEYQYEWVBKRPIXYGPETAJAEXQWOAOMMWOSFDOEXJFZAFORNZBE
UUBULTSMXRQLOFOFNZXTJPLGZMDTWULHCVELXLOYYTLZCOMTGPTSGPYBFBKAJGZAISOAHPJZC
AGBVMHPTIPZYBRNPTRLSOUADTTBQOQHRCWHYISOZEYBQUZURAHPICIPFBZEPAENMNKYKFXZTB
IOWAEPZLBIOPNQQYOBFKUDSMMKVECFOFETZPISZMTOSZBIKAHTALXZPGZMLGRUAXSMTLVOLIS
VLTJWFXJFXKIYOTTBIOHRNPPXAIKUDMMQUZHVHDYMDYNPBLVPVLYPFVVVPAENMBBYOHBSGBGV
PEDAZNMMYCEDIWYWURLBZEENIUSZSEIMRM
```

Η μορφή της εξόδου του προγράμματος θα πρέπει να είναι η εξής:

```
KEY1 PLAINTEXT1 IC1

KEY2 PLAINTEXT2 IC2

KEY3 PLAINTEXT3 IC3

KEY4 PLAINTEXT4 IC4
```

... (κ.ο.κ. συνολικά 10 το πολύ γραμμές αυτής της μορφής)

Σημείωση: άλλοι τρόποι λύσης γίνονται δεκτοί, ενδεχομένως με μειωμένη βαθμολογία, εφόσον τους αναφέρετε. Για παράδειγμα, η χρήση του online calculator του δείκτη σύμπτωσης που θα βρείτε εδώ: https://www.dcode.fr/index-coincidence. Η χρήση Vigenere solver δεν επιτρέπεται.

Λύση:

Ο κώδικας που υλοποιεί την παραπάνω συνάρτηση επισυνάπτεται στο zip αρχείο που υποβλήθηκε.

Προκύπτει το κλειδί "KHALILGIB".

Και το plaintext είναι:

"ANDAWOMANWHOHELDABABEAGAINSTHERBOSOMSAIDSPEAKTOUSOFCHILDRENANDHESAIDYOURC
HILDRENARENOTYOURCHILDRENTHEYARETHESONSANDDAUGHTERSOFLIFESLONGINGFORITSEL
FTHEYCOMETHROUGHYOUBUTNOTFROMYOUANDTHOUGHTHEYAREWITHYOUYETTHEYBELONGNOTTO
YOUYOUMAYGIVETHEMYOURLOVEBUTNOTYOURTHOUGHTSFORTHEYHAVETHEIROWNTHOUGHTSYOU
MAYHOUSETHEIRBODIESBUTNOTTHEIRSOULSFORTHEIRSOULSDWELLINTHEHOUSEOFTOMORROW
WHICHYOUCANNOTVISITNOTEVENINYOURDREAMSYOUMAYSTRIVETOBELIKETHEMBUTSEEKNOTT
OMAKETHEMLIKEYOUFORLIFEGOESNOTBACKWARDNORTARRIESWITHYESTERDAYYOUARETHEBOW
SFROMWHICHYOURCHILDRENASLIVINGARROWSARESENTFORTHTHEARCHERSEESTHEMARKUPONT
HEPATHOFTHEINFINITEANDHEBENDSYOUWITHHISMIGHTTHATHISARROWSMAYGOSWIFTANDFAR
LETYOURBENDINGINTHEARCHERSHANDBEFORGLADNESSFOREVENASHELOVESTHEARROWTHATFL
IESSOHELOVESALSOTHEBOWTHATISSTABLE"

Επεξήγηση:

Χρησιμοποιήθηκε η γλώσσα Python διότι προσφέρει ευκολία στην διαχείριση συμβολοσειρών. Για την εύρεση του κλειδιού χρησιμοποιήθηκε ο τύπος $r \approx \frac{I_{eng}-I_{rand}}{I_{text}-I_{rand}}$ ο οποίος δεν έβγαζε σωστό μήκος κλειδιού. Για αυτό το λόγο, παρατηρώντας τους IC των ομάδων που προέκυψαν φάνηκε ότι δεν ήταν καλοί. Έτσι, γίνεται έλεγχος όλων των τιμών γύρω από το r και συγκεκριμένα από το $1 – 2 \cdot r$, δηλαδή από 1 μέχρι 10 και τελικά προέκυψε η τιμή 9 είναι η καλύτερη. Έτσι, έχοντας πλέον το μήκος του κλειδιού, μπορούν να υπολογιστούν οι σχετικές ολισθήσεις με την δεύτερη ομάδα γραμμάτων που είχε δείκτη σύμπτωσης πολύ κοντά σε αυτόν της φυσικής γλώσσας. Έτσι, για όλες τις ομάδες γραμμάτων βρέθηκαν οι ολισθήσεις που δίνουν το καλύτερο IC. Τέλος, εκτυπώνονται οι 26 διαφορετικές εναλλακτικές για τα διαφορετικά κλειδιά και τα αντίστοιχα κείμενα.

5η Άσκηση

1. *Αποδείξτε ότι το κρυπτοσύστημα της διαφάνειας 21 (Lecture 1) δεν διαθέτει τέλεια μυστικότητα αν τα κλειδιά δεν είναι ισοπίθανα (δείξτε το με χρήση του ορισμού του Shannon, χωρίς χρήση των ισοδύναμων συνθηκών).*

2. *Σε ένα κρυπτοσύστημα που διαθέτει τέλεια μυστικότητα, είναι αναγκαίο κάθε κλειδί να επιλέγεται με την ίδια πιθανότητα; Έχει σημασία αν οι χώροι είναι ισοπληθικοί; Αποδείξτε τους ισχυρισμούς σας.*

3. *Να αποδείξετε ότι οι παρακάτω προτάσεις είναι ισοδύναμες με τη συνθήκη τέλειας μυστικότητας του Shannon:*

i) $\forall x \in M, y \in C : Pr[C = y] = Pr[C = y \mid M = x]$

ii) $\forall x_1, x_2 \in M, y \in C : Pr[C = y \mid M = x_1] = Pr[C = y \mid M = x_2]$

Λύση:

Σύμφωνα με τον ορισμό της τέλειας μυστικότητας, ένα κρυπτογραφικό σχήμα είναι τέλεια μυστικό στο χώρο των μηνυμάτων M αν για κάθε κατανομή πιθανότητας στο M, για κάθε μήνυμα $x \in M$ και κάθε κρυπτοκείμενο $y \in C$, για το οποίο ισχύει $Pr[C = y] > 0$: $Pr[M = x \mid C = y] = Pr[M = x]$.

1. Έστω το εξής κρυπτοσύστημα όπου $M = \{0, 1\}$, $C = \{A, B\}$ και $K = \{K_1, K_2\}$ με πιθανότητα $Pr[K_1] = 1/3$, $Pr[K_2] = 2/3$ ενώ τα αρχικά κείμενα είναι ισοπίθανα.

	K_1	K_2
0	A	B
1	B	A

Τότε,

$Pr[C = A] = Pr[K = K_1 \wedge M = 0] + Pr[K = K_2 \wedge M = 1] \Rightarrow$

$Pr[C = A] = \frac{1}{3} * \frac{1}{2} + \frac{2}{3} * \frac{1}{2} = \frac{1}{2}$

$Pr[C = B] = Pr[K = K_1 \wedge M = 1] + Pr[K = K_2 \wedge M = 0] \Rightarrow$

$Pr[C = B] = \frac{1}{3} * \frac{1}{2} + \frac{2}{3} * \frac{1}{2} = \frac{1}{2}$

Έπειτα, για τον υπολογισμό της πιθανότητας $Pr[M = x \mid C = y]$ για $x = 0$ και $y = A$ με τον Νόμο του Bayes, προκύπτει το εξής:

$$Pr[M = 0 \mid C = A] = \frac{Pr\,[C=A|M=0] * Pr\,[M=0]}{Pr\,[C=A]} = \frac{Pr[K=K_1] * \frac{1}{2}}{\frac{1}{2}} = \frac{1}{3}$$

Παρομοίως, για την πιθανότητα $Pr[M = x \mid C = y]$ για $x = 0$ και $y = B$ προκύπτει ότι:

$$Pr[M = 0 \mid C = B] = \frac{Pr\,[C=B|M=0] * Pr\,[M=0]}{Pr\,[C=B]} = \frac{Pr[K=K_2] * \frac{1}{2}}{\frac{1}{2}} = \frac{2}{3}$$

2. Παρακάτω αποδεικνύεται ότι η τέλεια μυστικότητα ισχύει και για μη ισοπίθανα κλειδιά.

Υπάρχει το εξής αντιπαράδειγμα. Έστω το εξής κρυπτοσύστημα όπου M = {0, 1}, C = {A, B} και K = {K_1, K_2, K_3} με πιθανότητα Pr[K_1] = ½ , Pr[K_2] = ¼ , Pr[K_3] = ¼ ενώ τα αρχικά κείμενα είναι ισοπίθανα.

	K_1	K_2	K_3
0	A	B	B
1	B	A	A

Τότε,

Pr[C = A] = Pr[K = K_1 ∧ M = 0] + Pr[K = K_2 ∧ M = 1] + Pr[K = K_3 ∧ M = 1] ⇒

$$\Pr[C = A] = \frac{1}{2} * \frac{1}{2} + \frac{1}{4} * \frac{1}{2} + \frac{1}{4} * \frac{1}{2} = \frac{1}{2}$$

Pr[C = B] = Pr[K = K_1 ∧ M = 1] + Pr[K = K_2 ∧ M = 0] + Pr[K = K_3 ∧ M = 0] ⇒

$$\Pr[C = B] = \frac{1}{2} * \frac{1}{2} + \frac{1}{4} * \frac{1}{2} + \frac{1}{4} * \frac{1}{2} = \frac{1}{2}$$

Έπειτα, για τον υπολογισμό της πιθανότητας Pr[M = x | C = y] για x = 0 και y = A με τον Νόμο του Bayes, προκύπτει το εξής:

$$\Pr[M = 0 \mid C = A] = \frac{\Pr[C=A|M=0] * \Pr[M=0]}{\Pr[C=A]} = \frac{\Pr[K=K_1] * \frac{1}{2}}{\frac{1}{2}} = \frac{1}{2} = \Pr[M = 1]$$

Παρομοίως, για την πιθανότητα Pr[M = x | C = y] για x = 0 και y = B προκύπτει ότι:

$$\Pr[M = 0 \mid C = B] = \frac{\Pr[C=B|M=0] * \Pr[M=0]}{\Pr[C=B]} = \frac{(\Pr[K=K_1] + \Pr[K=K_3]) * \frac{1}{2}}{\frac{1}{2}} = \frac{1}{2} = \Pr[M = 1]$$

Παρομοίως, μπορεί να δειχθεί και για x = 1.

Επομένως, ισχύει ότι για Pr[M = x | C = y] = Pr[M = x], χωρίς να είναι απαραίτητο η κατανομή των κλειδιών να είναι ομοιόμορφη.

Εναλλακτικά, από την τέλεια μυστικότητα κατά Shannon προκύπτει ότι το κρυπτοκείμενο δεν δίνει καμία πληροφορία για το ποιο είναι το αρχικό κείμενο. Μάλιστα, αν τα κλειδιά δεν επιλέγονται με την ίδια πιθανότητα τότε για ένα δοσμένο κρυπτοκείμενο υπάρχει κάποιο κείμενο που έχει μεγαλύτερη πιθανότητα και αυτό συμβαίνει διότι το αντίστοιχο κλειδί που τα συνδέει θα έχει μεγαλύτερη πιθανότητα και για αυτό το λόγο είναι τελικά απαραίτητο τα κλειδιά να είναι ισοπίθανα.

3. (i) Ευθύ: Αποδεικνύεται ότι αν $\forall x \in M, y \in C : Pr[C = y] = Pr[C = y \mid M = x]$, τότε θα ισχύει η συνθήκη τέλειας μυστικότητας του Shannon.

Αρχικά, από την σχέση τέλειας μυστικότητας ισχύει:

$Pr[M = x \mid C = y] = Pr[M = x]$

Έπειτα, από τον Νόμο του Bayes ισχύει:

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

$Pr[M = x] = Pr[M = x \mid C = y]$

Και, με απαλοιφή των κοινών όρων και πολλαπλασιασμό με $Pr[C = y]$, προκύπτει η ζητούμενη σχέση.

Αντίστροφο: Παρομοίως, αποδεικνύεται ότι αν ισχύει η τέλεια μυστικότητα κατά Shannon, τότε θα ισχύει $\forall x \in M, y \in C : Pr[M = x] = Pr[M = x \mid C = y]$.

Έτσι, $Pr[M = x \mid C = y] = \frac{Pr[C=y|M=x] * Pr[M=x]}{Pr[C=y]} \Rightarrow Pr[M = x] = \frac{Pr[C=y|M=x] * Pr[M=x]}{Pr[C=y]} \Rightarrow$

$Pr[C = y] = Pr[C = y \mid M = x]$

(ii) Ευθύ: Αν $\exists$ τέλεια μυστικότητα, τότε $\forall x_1, x_2 \in M, y \in C: Pr[C = y \mid M = x_1] = Pr[C = y \mid M = x_2]$.

1ος τρόπος:

Αρχικά, λόγω τέλειας μυστικότητας θα ισχύει ότι για κάθε x_i: $Pr[M = x_i \mid C = y] = Pr[M = x_i]$

Από το βήμα (i) ισχύει ότι: $Pr[C = y \mid M = x_i] = Pr[C = y] = \delta_y$

Άρα, αφού η δ_y είναι μια σταθερά που εξαρτάται μόνο από το κρυπτοκείμενο y, για κάθε x, x' θα ισχύει: $Pr[C = y \mid M = x] = \delta_y = Pr[C = y \mid M = x']$

2ος τρόπος:

Ζητείται να δειχθεί ότι η τέλεια μυστικότητα συνεπάγεται $Pr[M = x \mid C = y] = Pr[M = x]$.

Όπως αποδείχθηκε στο βήμα (i) οι 2 προτάσεις είναι ισοδύναμες άρα μπορεί να γράψει κανείς ότι:

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

Άρα, για οποιαδήποτε 2 κείμενα θα ισχύει:

$Pr[C = y \mid M = x_1] = Pr[C = y \mid M = x_2] = Pr[C = y]$

Αντίστροφο: Αν ισχύει ότι $\forall\, x_1, x_2 \in M, y \in C : Pr[C = y \mid M = x_1] = Pr[C = y \mid M = x_2]$, τότε θα ισχύει και τέλεια μυστικότητα.

1ος τρόπος:

Έστω το αρχικό κείμενο x για το οποίο ισχύει ότι $Pr[C = y \mid M = x] = \delta_y$. Τότε, για όλα τα αρχικά κείμενα x' θα ισχύει $Pr[C = y \mid M = x'] = \delta_y$.

Έτσι, $Pr[M = x \mid C = y] = \frac{Pr[C=y|M=x]*Pr[M=x]}{Pr[C=y]} = \frac{Pr[C=y|M=x]*Pr[M=x]}{\sum_{x' \in M} Pr[C=y|M=x']*Pr[M=x']} = \frac{\delta_y * Pr[M=x]}{\sum_{x' \in M} \delta_y * Pr[M=x']} =$

$= \frac{Pr[M=x]}{\sum_{x' \in M} Pr[M=x']}$

Και επειδή το άθροισμα ισούται με 1, αφού είναι άθροισμα πάνω στην πιθανότητα όλων των αρχικών κειμένων, θα ισχύει: $Pr[M = x \mid C = y] = Pr[M = x]$

2ος τρόπος:

Έστω ότι όλες οι πιθανότητες είναι ίσες με δ.

Ισχύει ότι, $Pr[C = y, M = x_1] = Pr[C = y \mid M = x_2] * Pr[M = x_1]$

Άρα, $Pr[M = x_1 \mid C = y] = \frac{Pr[C=y,M=x_1]}{Pr[C=y]} = \frac{Pr[C=y|M=x_2]*Pr[M=x_1]}{Pr[C=y]} = Pr[M = x_1]$

Δεδομένου ότι, $\sum_{x_i \in M} Pr[M = x_i] = 1$

$Pr[C = y] = \sum_{x_i \in M} Pr[C = y|M = x_i] * Pr[M = x_i] = \sum_{x_i \in M} \delta * Pr[M = x_i] = \delta$

Resources:

1. *Διαφάνειες Μαθήματος*
2. *https://theory.stanford.edu/~jvondrak/MATH233B-2017/lec3.pdf*
3. *Paul D. Humke: Lagrange's Theorem: Statement and Proof, April 5, 2012*
4. *Keith Conrad: Cosets and Lagrange's Theorem, The Miller-Rabin Test*
5. *Marek Cygan, Fedor V. Fomin, Lukasz Kowalik, Daniel Lokshtanov, Dániel Marx, Marcin Pilipczuk, Michal Pilipczuk, and Saket Saurabh. Parameterized Algorithms. Springer, 2016.*
6. *Douglas R. Stinson, Maura B.Patterson. Cryptography Theory and Practice, Fourth Edition. CRC Press, 2019*
7. *Fomin, F.V., Kaski, P.: Exact exponential algorithms. Communications of the ACM 56(3), 80-88*
8. *F.V. Fomin, M. Pilipczuk, etc: Kernelization and Sparseness: the case of Dominating Set*
9. *WolframAlpha. Average English Word*
10. *https://www.nku.edu/~christensen/1402%20Friedman%20test%202.pdf*
11. *Quist-Aphetsi Kester. A cryptosystem based on Vigenère cipher with varying key. International Journal of Advanced Research in Computer Engineering & Technology, 2012*
12. *http://facweb1.redlands.edu/fac/Tamara_Veenstra/cryptobook/Attack-Viggy.html?fbclid=IwAR2r4j3B_i2XFZoNWpI6UEWz9j2IAyBClmP3e9quE9_GKE3iwz1NBo2sW0U*