ΟΙΚΟΝΟΜΙΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΜΑΘΗΜΑ: ΚΡΥΠΤΟΓΡΑΦΙΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ, 2013
ΔΙΔΑΣΚΩΝ: Ε. Μαρκάκης

1η Σειρά Ασκήσεων

Σκοπός της εργασίας αυτής είναι η εξοικείωση με τις κρυπταναλυτικές τεχνικές για στοιχειώδη κρυπτοσυστήματα, όπως ο κώδικας Vigenère.

Μέρος Α: Χωριστείτε σε ομάδες των 2 (όσοι θέλουν μπορούν να δουλέψουν και ατομικά για την άσκηση αυτή). Κάθε ομάδα θα κρυπτογραφήσει ένα κείμενο με αγγλικούς χαρακτήρες χρησιμοποιώντας τον κώδικα Vigenère. Κάθε ομάδα είναι ελεύθερη να επιλέξει το κείμενο που θα κρυπτογραφήσει και το κλειδί, αρκεί να πληρούνται οι εξής προϋποθέσεις:

1) Το κείμενο θα πρέπει να έχει τουλάχιστον 400 χαρακτήρες και το πολύ 800.
2) Το κλειδί που θα επιλεξετε θα έχει μήκος από 4 έως 9 χαρακτήρες. Κάθε ομάδα θα διατηρήσει μυστικό το κλειδί καθώς και το μήκος του.
3) Δεν θα κρυπτογραφήσετε κενά, σημεία στίξης, αριθμούς, ή άλλους χαρακτήρες εκτός των 26 κεφαλαίων χαρακτήρων του λατινικού αλφαβήτου. Για ομοιομορφία, θα μετατρέψετε το αρχικό κείμενο ώστε να έχει μόνο κεφαλαία γράμματα. Επομένως το plaintext που θα κρυπτογραφήσετε θα είναι ένα συνεχές string, που θα προκύψει αφού αφαιρέσετε τα κενά και τα σημεία στίξης (αν το κείμενο έχει αριθμούς μπορείτε να τους γράψετε ολογράφως). Το τελικό cihertext θα είναι επίσης ένα συνεχές string χαρακτήρων χωρίς κενά, όπως και τα παραδείγματα που είδαμε στις σχετικές διαλέξεις.
4) Είναι προτιμότερο να μην χρησιμοποιήσετε κάποιο τεχνικό κείμενο ως plaintext. Μπορείτε να χρησιμοποιήσετε κείμενο από κάποιο λογοτεχνικό βιβλίο, ή από περιοδικά ή εφημερίδες. Μην χρησιμοποιήσετε «τυχαίο» κείμενο (δηλ. με βάση κάποια γεννήτρια τυχαίων αριθμών).

Η προθεσμία για το Μέρος Α είναι την **Τρίτη, 19/11/2013**. Για την παράδοση, που γίνεται μέσω του eclass, θα πρέπει να στείλετε ένα αρχείο zip, που θα περιέχει 2 αρχεία txt: ένα με το plaintext (το οποίο θα έχει και το κλειδί στην τελευταία γραμμή), και ένα που θα έχει μόνο το ciphertext. Προαιρετικά μπορείτε να βάλετε και επιπλέον αρχεία με τον κώδικα που χρησιμοποιήσατε και επεξηγήσεις ως προς την υλοποίησή σας.

Μέρος Β: Στο 2ο μέρος κάθε ομάδα θα λάβει ένα ciphertext, που θα έχει παραχθεί από κάποια άλλη ομάδα, και θα προσπαθήσει να το αποκρυπτογραφήσει χρησιμοποιώντας τη μέθοδο Kasiski αλλά και τη μέθοδο με τον υπολογισμό του δείκτη σύμπτωσης (index of coincidence) που είδαμε στο μάθημα. Θα εφαρμόσετε αρχικά και τις 2 μεθόδους για να μαντέψετε το μήκος του κλειδιού. Ακόμα κι αν είστε σίγουροι από την 1η μέθοδο για το μήκος του κλειδιού, θα εφαρμόσετε και τη 2η για

επαλήθευση. Στη συνέχεια, θα χρειαστείτε επίσης να αποκρυπτογραφήσετε μονοαλφαβητικές αντικαταστάσεις, για τις οποίες μπορείτε να χρησιμοποιήσετε τα στατιστικά για τη συχνότητα εμφάνισης κάθε χαρακτήρα στην αγγλική γλώσσα, που υπάρχουν στις διαφάνειες. Παραδοτέο της κάθε εργασίας θα είναι ο κώδικας που θα γράψετε καθώς και μία αναφορά (σε αρχείο PDF) όπου θα εξηγήσετε τη διαδικασία που ακολουθήσατε για την αποκρυπτογράφηση. Ακόμα και αν δεν μπορέσετε να αποκρυπτογραφήσετε όλο το κείμενο, περιγράψτε τη μεθοδολογία και τις δοκιμές που κάνατε.

Η προθεσμία για το Μέρος Β είναι την **Κυριακή, 15/12/2013** (παράδοση στο eclass).