ΕΠΛ326: Εργαστήριο 1
Απλοί αλγόριθμοι κρυπτογράφησης

Εισαγωγή

Στο σημερινό εργαστήριο θα ασχοληθούμε με απλούς αλγόριθμους κρυπτογράφησης (ciphers). Θα σας δοθεί η ευκαιρία να κρυπτογραφήσετε και να αποκρυπτογραφήσετε μηνύματα κειμένου. Για την κρυπτογράφηση και αποκρυπτογράφηση των μηνυμάτων, μπορείτε να γράψετε μικρά προγράμματα (scripts).

Εκτέλεση Εργαστηρίου

ΒΗΜΑ 1

Υπολογίστε τις πιο κάτω πράξεις χωρίς να χρησιμοποιήσετε υπολογιστές ή το Google.

(1) 5*2 mod 9 1
(2) 7*9 mod 11 8
(3) -11*3 mod 13 6
(4) 10*2 mod 2 0
(5) 11*3 mod 2 1

ΒΗΜΑ 2

Υποθέστε ότι έχετε ένα αλφάβητο με 10 διαφορετικούς χαρακτήρες και *ιδανική κρυπτογράφηση αντικατάστασης* (ideal substitution cipher). Πόσο μεγάλος είναι ο χώρος των κλειδιών; 10!

ΒΗΜΑ 3

Δημιουργήστε ένα πρόγραμμα το οποίο θα κρυπτογραφεί και θα αποκρυπτογραφεί μηνύματα με βάση τον αλγόριθμο Caesar. Θα χρησιμοποιήσετε το αγγλικό αλφάβητο (πεζά γράμματα) και το πρόγραμμα θα παίρνει ως είσοδο το κλειδί *K* και το μήνυμα που θα κρυπτογραφήσει, *M*. Το πρόγραμμα μπορείτε να το γράψετε σε Python, Java ή Ruby.

ΒΗΜΑ 4

Δημιουργήστε ένα πρόγραμμα το οποίο θα κρυπτογραφεί και θα αποκρυπτογραφεί μηνύματα με τη βοήθεια μετατοπίσεων (transpositions). Θα χρησιμοποιήσετε το αγγλικό αλφάβητο (πεζά γράμματα) και το πρόγραμμά σας θα παίρνει ως είσοδο το κλειδί *K* και το μήνυμα που θα κρυπτογραφήσει, *M*. Το πρόγραμμά σας θα υποθέτει ότι το μήνυμα μπαίνει σε ένα πίνακα με γραμμές μεγέθους *K*. Το αποτέλεσμα της κρυπτογράφησης θα προκύπτει από την ανάγνωση του ανάστροφου πίνακα (δείτε παράδειγμα πιο κάτω). Το πρόγραμμα μπορείτε να το γράψετε σε Python, Java ή Ruby.

Ακολουθεί ένα σχηματικό παράδειγμα λειτουργίας για *M*="cryptographyrocks" και *K*=3. Αρχικά θεωρούμε το μήνυμα ότι είναι ένας μονοδιάστατος πίνακας,

cryptography = [c, r, y, p, t, o, g, r, a, p, h, y, r, o, c, k, s],

στη συνέχεια τον κάνουμε δισδιάστατο με αριθμό στηλών ίσο με *K,*

[c, r, y, p, t, o, g, r, a, p, h, y, r, o, c, k, s] = [[c, r, y], [p, t, o], [g, r, a], [p, h, y], [r, o, c], [k, s, **0**]],

προσέξτε ότι έχουμε προσθέσει έναν επιπρόσθετο χαρακτήρα (το 0), το οποίο λέγεται και *padding,* ώστε να έχουμε τρεις στήλες (όσο είναι το κλειδί) σε κάθε γραμμή. Στη συνέχεια, κρυπτογραφούμε τον πίνακα, υπολογίζοντας τον ανάστροφό του (δηλ., οι στήλες γίνονται γραμμές και οι γραμμές στήλες),

[["**c**", "p", "g", "p", "r", "k"], ["**r**", "t", "r", "h", "o", "s"], ["**y**", "o", "a", "y", "c", "0"]]

δείτε, για παράδειγμα, τους χαρακτήρες που είναι έντονοι (bold), οι οποίοι προέρχονται από την πρώτη γραμμή του αρχικού πίνακα, άλλα είναι η πρώτη στήλη του τελικού πίνακα. Το αποτέλεσμα της κρυπτογράφησης, θα είναι ο παραπάνω πίνακας, σε μία διάσταση:

cpgprkrtrhosyoayc0

Με αντίστοιχη διαδικασία, θα πρέπει το πρόγραμμα να αποκρυπτογραφεί ένα μήνυμα.

ΒΗΜΑ 5

Σας δίνονται τα ακόλουθα κρυπτογραφημένα μηνύματα. Μπορείτε να υπολογίσετε τι κρύβουν; Προσέξτε αρχικά ότι τα μηνύματα έχουν πιο πλούσιο αλφάβητο από αυτό που έχετε χρησιμοποιήσει μέχρι στιγμής (πεζοί αγγλικοί χαρακτήρες). Είναι σημαντικό να θεωρήσετε το σωστό αλφάβητο ώστε να αποκρυπτογραφήσετε τα μηνύματα με επιτυχία. Το κενό (space) μπορεί να θεωρηθεί ότι είναι ένας επιπρόσθετος χαρακτήρας.

Ciphertext	Plaintext	Cipher and Key
`! almv !h!pwatlhjmh! aleqvohpizlmz`		
waymiwx dxjiylaivbpndrrig!ayxx		
snf r!tt riy0usuonp0d vc t0eoykco0		