2η Ατομική Εργασία

Ασκήσεις Συμμετρικής Κρυπτογραφίας

Υλοποιήστε μια επίθεση κρυπτανάλυσης η οποία θα εκμεταλλεύεται την κακή χρήση του cipher one-time-pad (OTP).

Σενάριο πρώτο (1 βαθμός)

Δυο ciphertexts C1 και C2 έχουνε δημιουργηθεί χρησιμοποιώντας την ίδια τυχαία ακολουθία. Για το ένα ciphertext γνωρίζετε το αντίστοιχο plaintext. Η επίθεση θα βρίσκει το 2^{o} plaintext.

- Το πρόγραμμα που θα υλοποιεί την επίθεση θα δέχεται τα ciphertext σε δυαδική μορφή.
- Θεωρούμε ότι η κωδικοποίηση των μηνυμάτων είναι ASCII.
- Η επίθεση να εφαρμόζεται ακόμα κι αν τα μηνύματα δεν έχουν το ίδιο μήκος. Διακρίνετε περιπτώσεις

Σενάριο δεύτερο (2 βαθμοί)

Δυο ciphertexts C1 και C2 έχουνε δημιουργηθεί χρησιμοποιώντας την ίδια τυχαία ακολουθία. Και για τα δυο plaintext έχετε κάποιες πληροφορίες που μπορείτε να χρησιμοποιήσετε για να τα βρείτε.

- Παραδοχές για τα μηνύματα:
    A. Και τα δύο μηνύματα είναι μόνο δεκαδικοί αριθμοί.
    B. Το ένα μήνυμα είναι μόνο δεκαδικοί αριθμοί και το άλλο μόνο γράμματα της αγγλικής γλώσσας.
- Το πρόγραμμα που θα υλοποιεί την επίθεση θα δέχεται τα ciphertext σε δυαδική μορφή.
- Θεωρούμε ότι η κωδικοποίηση των μηνυμάτων είναι ASCII.
- Η επίθεση να εφαρμόζεται ακόμα κι αν τα μηνύματα δεν έχουν το ίδιο μήκος.
- Προσοχή! Σε μερικές περιπτώσεις μπορεί να υπάρχουν περισσότερες από μια σωστές απαντήσεις.