Συμμετρική Κρυπτογραφία

Υλοποιήση μιας επίθεσης κρυπτανάλυσης η οποία θα εκμεταλλεύεται την κακή χρήση του cipher one-time-pad (OTP) (ή ενός stream cipher). Θα θεωρήσουμε ότι το η ίδια δυαδική ακολουθία (είτε η τυχαία του OTP είτε η έξοδο της γεννήτριας του stream cipher) χρησιμοποιείται για την προστασία μηνυμάτων.

Σενάριο πρώτο

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

- Το πρόγραμμα που θα υλοποιεί την επίθεση θα δέχεται τα ciphertext σε δυαδική μορφή και το γνωστό κείμενο σαν string. Θα επιστρέφει το άγνωστο μήνυμα σε string.
- Θεωρούμε ότι η κωδικοποίηση των μηνυμάτων σε δυαδική μορφή θα είναι με ASCII.
- Η επίθεση να εφαρμόζεται ακόμα κι αν τα μηνύματα δεν έχουν το ίδιο μήκος. Διακρίνετε περιπτώσεις

Σενάριο δεύτερο

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.

Θα θεωρήσουμε ότι τα μηνύματα είναι δεκαδικοί αριθμοί.

- 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. Διερευνείστε αν θα βοηθούσε και πως η ύπαρξη κι άλλων ciphertexts που έχουνε δημιουργηθεί χρησιμοποιώντας την ίδια τυχαία ακολουθία (προφανώς για άλλα plaintexts δεκαδικούς αριθμούς).