Πανεπιστήμιο Δυτικής Μακεδονίας
Πολυτεχνική Σχολή
Τμήμα Μηχανικών Πληροφορικής και Τηλεπικοινωνιών

Ασφάλεια Υπολογιστών και Δικτύων

1η Προαιρετική Εργαστηριακή Άσκηση

1. Υλοποίηση του (εκπαιδευτικού) αλγόριθμου συμμετρικής κρυπτογράφησης Simple DES

Στην παρούσα άσκηση θα πρέπει να υλοποιηθεί ο αλγόριθμος συμμετρικής κρυπτογράφησης SDES σε λειτουργίες κρυπτογράφησης και αποκρυπτογράφησης καθώς και ένα σενάριο βίαιης επίθεσης σε γλώσσα προγραμματισμού της επιλογής σας (ενδείκνυται η C). Συγκεκριμένα θα πρέπει να υλοποιηθούν τα εξής:

Διαδικασία κρυπτογράφησης:

Α) Εισαγωγή του απλού μηνύματος από το χρήστη είτε σε δυαδική είτε σε δεκαδική μορφή (8-bit).
Β) Εισαγωγή του κλειδιού κρυπτογράφησης (10-bit) από το χρήστη είτε σε δυαδική είτε σε δεκαδική μορφή.
Γ) Κρυπτογράφηση του απλού μηνύματος και εμφάνιση του κρυπτογραφήματος (8-bit) είτε σε δυαδική είτε σε δεκαδική μορφή.

Διαδικασία αποκρυπτογράφησης:

Α) Εισαγωγή του κρυπτογραφήματος από το χρήστη είτε σε δυαδική είτε σε δεκαδική μορφή (8-bit).
Β) Εισαγωγή του κλειδιού κρυπτογράφησης (10-bit) από το χρήστη είτε σε δυαδική είτε σε δεκαδική μορφή.
Γ) Αποκρυπτογράφηση του κρυπτογραφήματος και εμφάνιση του απλού μηνύματος (8-bit) είτε σε δυαδική είτε σε δεκαδική μορφή.

Διαδικασία βίαιης επίθεσης

Α) Εισαγωγή ενός αρχικού μηνύματος (8-bit) και ενός κρυπτογραφήματος (8-bit) από τον χρήστη είτε σε δυαδική είτε σε δεκαδική μορφή.
Β) Βίαιη αναζήτηση του κλειδιού κρυπτογράφησης και εμφάνισή του (10-bit). Εάν υπάρχουν περισσότερα από ένα κλειδιά κρυπτογράφησης να εμφανίζονται όλα.
Γ) Εξαγωγή του μέσου χρόνου επιτυχημένης αναζήτησης σε N προσπάθειες, N > 10.

Παραδοτέα:

Η παράδοση της άσκησης θα γίνει μέσω eclass. Παραδοτέα αρχεία:

1. Ένα αρχείο κειμένου sdes_A.M.pdf, όπου Α.Μ. ο αριθμός μητρώου, στο οποίο θα παρουσιάζεται ο τρόπος ανάπτυξης του κώδικα.

2. Το αρχείο του κώδικα, στο οποίο θα περιέχονται αναλυτικά σχόλια λειτουργίας και εκτέλεσης.

Να προσεχθούν:

1. Στο αρχείο κειμένου να αναγράφεται το ονοματεπώνυμό σας, το εξάμηνό σας και ο αριθμός μητρώου σας.
2. Για την καταγραφή του χρόνου αναζήτησης του κλειδιού στην 3η διαδικασία μπορείτε να χρησιμοποιήσετε την συνάρτηση gettimeofdate() που επιστρέφει με ακρίβεια τον χρόνο αναζήτησης.