Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

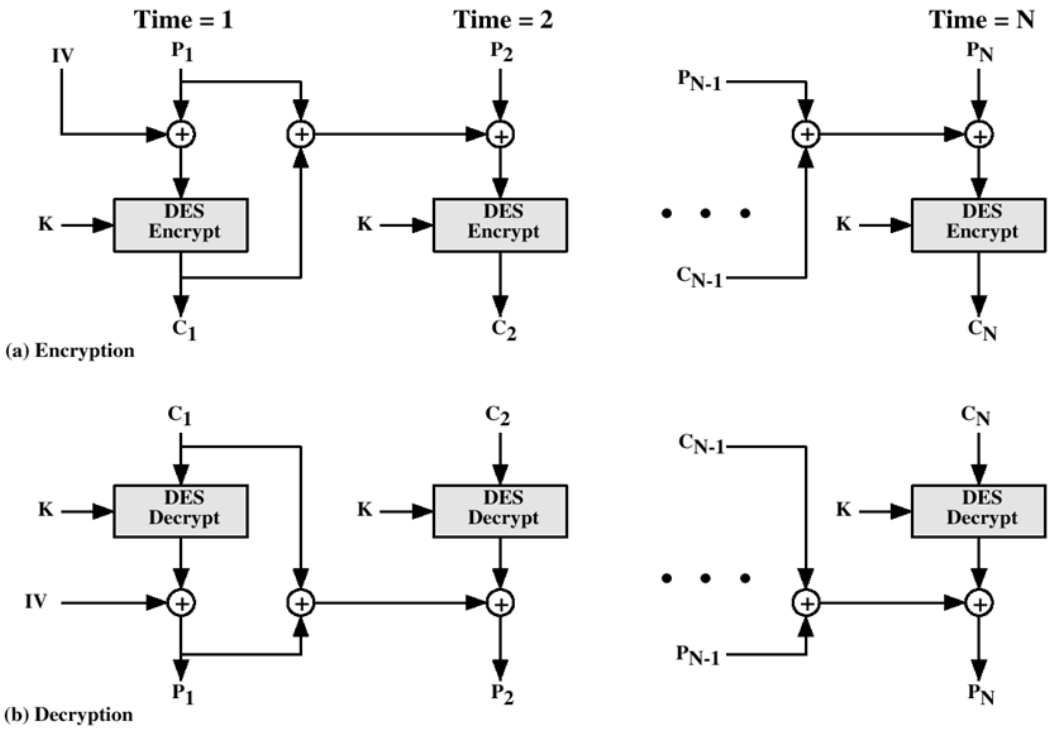
Εργαστήριο Ηλεκτρονικών Κυκλωμάτων, Συστημάτων και Εφαρμογών (ECSA Lab.)

Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος (Καθηγητής)

Ασκήσεις στη θεματική ενότητα του Kerberos

1) Να δείξετε ότι με τη μέθοδο PCBC ένα τυχαίο λάθος σε ένα τμήμα του κρυπτογραφήματος διαδίδεται σε όλα τα ακόλουθα τμήματα του αρχικού κειμένου.



2) Υποθέστε ότι με τη μέθοδο PCBC ανταλλάσσονται κατά τη διάρκεια μια μεταφοράς τα τμήματα C_i και C_{i+1} . Να δείξετε ότι αυτό επηρεάζει μόνο τα κρυπτογραφημένα τμήματα P_i και P_{i+1} αλλά όχι τα επακόλουθα τμήματα.