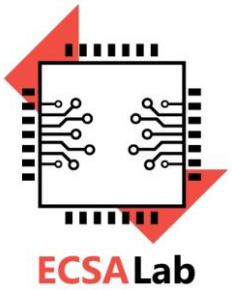
Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου

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

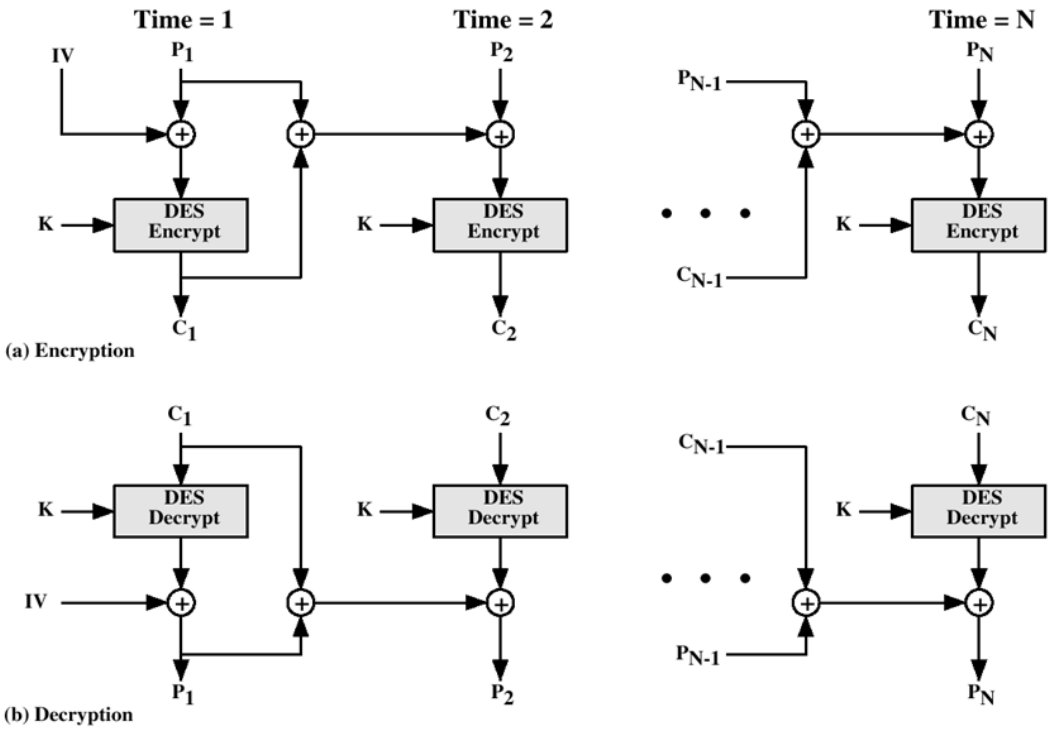


Ασφάλεια Υπολογιστικών Συστημάτων

Διδάσκων: Δρ. Παρασκευάς Κίτσος

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.



ΛΥΣΗ:

Έστω ένα λάθος στο κρυπτογράφημα C_1 το οποίο επηρεάζει το P_1 (αρχικό μήνυμα) γιατί η αποκρυπτογράφηση του C_1 υφίσταται XOR με το IV για τα δημιουργηθεί το P_1. Μαζί τα C_1 και P_1 επηρεάζουν το P_2 γιατί μεταξύ τους υφίσταται XOR και το αποτέλεσμα υφίσταται XOR με την αποκρυπτογράφηση του C_2 . Παρόμοια ισχύει για κάθε κρυπτογράφημα και για τα επόμενά του τμήματα αρχικού κειμένου.

2) Υποθέστε ότι με τη μέθοδο PCBC ανταλλάσσεται η σειρά, κατά τη διάρκεια μιας μεταφοράς, των τμημάτων 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.

ΛΥΣΗ:

Έστω η περίπτωση της ανταλλαγής των C_1 και C_2 . Ότι συμπεράσματα εξαχθούν θα ισχύουν για δύο οποιαδήποτε διαδοχικά τμήματα. Αρχικά έστω ότι τα C_1 και C_2 μεταφέρονται με την ορθή σειρά. Τότε θα έχουμε κατά την αποκρυπτογράφηση.

$$P_1 = E[K, C_1] \oplus IV$$
$$P_2 = E[K, C_2] \oplus C_1 \oplus P_1 = E[K, C_2] \oplus C_1 \oplus E[K, C_1] \oplus IV$$
$$P_3 = E[K, C_3] \oplus C_2 \oplus P_2 = E[K, C_3] \oplus C_2 \oplus E[K, C_2] \oplus C_1 \oplus E[K, C_1] \oplus IV$$

Έστω τώρα ότι τα τμήματα C_1 και C_2 μεταφέρονται με την ανάποδη σειρά. Αν συμβολίσουμε με Q_i τα αποκρυπτογραφημένα τμήματα θα έχουμε.

$$Q_1 = E[K, C_2] \oplus IV$$
$$Q_2 = E[K, C_1] \oplus C_2 \oplus Q_1 = E[K, C_1] \oplus C_2 \oplus E[K, C_2] \oplus IV$$
$$Q_3 = E[K, C_3] \oplus C_1 \oplus Q_2 = E[K, C_3] \oplus C_1 \oplus E[K, C_1] \oplus C_2 \oplus E[K, C_2] \oplus IV$$

Παρατηρούμε ότι τα Q_1 και Q_2 είναι διαφορετικά από τα P_1 και P_2 αλλά το Q_3 είναι ίδιο με το P_3. Άρα επηρεάζονται μόνο τα αντίστοιχα τμήματα.