ΤΕΙ ΚΕΝΤΡΙΚΗΣ ΜΑΚΕΔΟΝΙΑΣ

ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΙΚΑ ΜΑΘΗΜΑΤΑ

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ(Θ)

Ενότητα 4: ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

ΔΙΔΑΣΚΩΝ: ΚΩΝΣΤΑΝΤΙΝΟΣ ΧΕΙΛΑΣ

ΣΧΟΛΗ ΤΕΧΝΟΛΟΓΙΚΩΝ ΕΦΑΡΜΟΓΩΝ
ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ
ΤΕ

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο

ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ

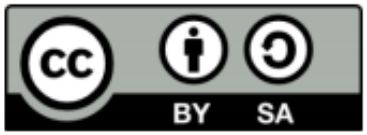
ΕΣΠΑ 2007-2013
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Άδειες Χρήσης

- Το παρόν εκπαιδευτικό υλικό υπόκειται σε άδειες χρήσης Creative Commons.

- Για εκπαιδευτικό υλικό, όπως εικόνες, που υπόκειται σε άλλου τύπου άδειας χρήσης, η άδεια χρήσης αναφέρεται ρητώς.



Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «Ανοικτά Ακαδημαϊκά Μαθήματα στο ΤΕΙ Κεντρικής Μακεδονίας» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Ενότητα 4

ΑΣΦΑΛΕΙΑ & ΔΙΑΧΕΙΡΙΣΗ ΔΙΚΤΥΩΝ

Χειλάς Κωνσταντίνος
Διδάκτορας Φυσικής

Περιεχόμενα ενότητας

1. Τρόποι κρυπτογράφησης
2. Electronic Code Book Problem
3. Cipher Block Chaining
4. Cipher Feedback Mode
5. Cipher Feedback Mode κρυπτογράφηση
6. Cipher Feedback Mode αποκρυπτογράφηση
7. Stream Cipher Mode
8. Παράδειγμα keystream reuse attack
9. WEP (γιατί δεν είναι κατάλληλο;)
10. Counter mode
11. Αλγόριθμοι συμμετρικού κλειδιού
    1. Διανομή κλειδιών

Σκοποί ενότητας

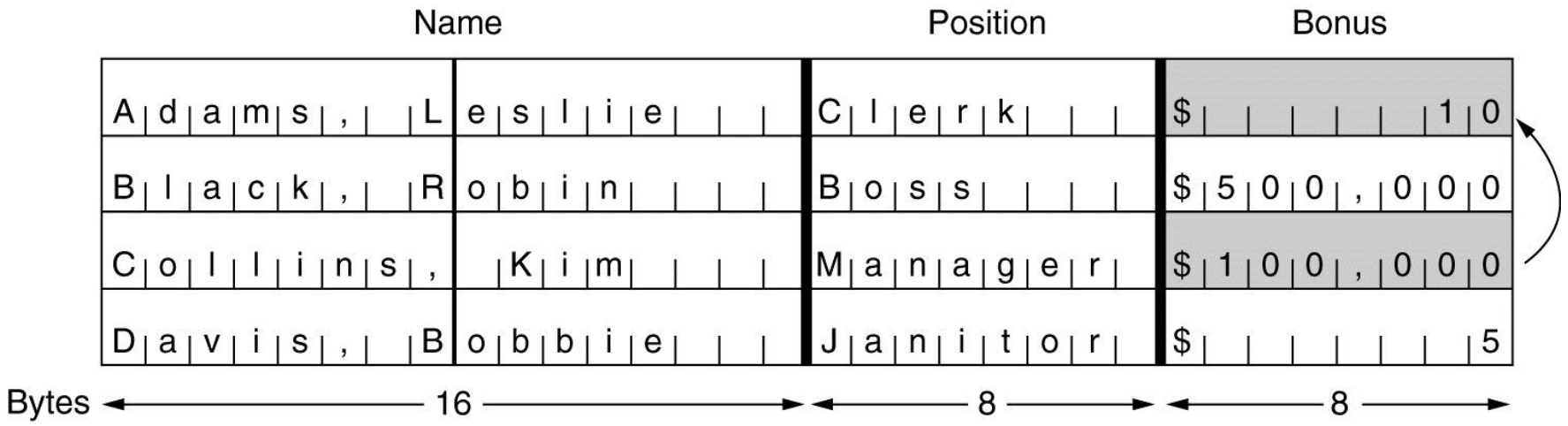
Αλγόριθμοι συμμετρικού κλειδιού

Καταστάσεις/ τρόποι κρυπτογράφησης (Cipher Modes)

Τρόποι κρυπτογράφησης

- Όλοι οι block ciphers είναι στην ουσία μονοαλφαβητικοί κώδικες αντικατάστασης απλά χρησιμοποιούν πιο μεγάλους χαρακτήρες (64 ή 128 Bit)
- Όσες φορές κι αν κωδικοποιήσω το ίδιο κομμάτι κειμένου χρησιμοποιώντας το ίδιο κλειδί, το αποτέλεσμα θα είναι το ίδιο.
- Electronic Code Book (ECB)
- Σε μηνύματα που είναι δομημένα ο κρυπταναλυτής μπορεί να βρει στοιχεία για να αλλοιώσει ή να αντικαταστήσει το περιεχόμενο κάποιων κομματιών.
- Ο στόχος είναι να υπάρχει τρόπος ώστε αν υπάρξουν όμοια κομμάτια κειμένου αυτά να δώσουν διαφορετικά κωδικοποιημένα blocks.

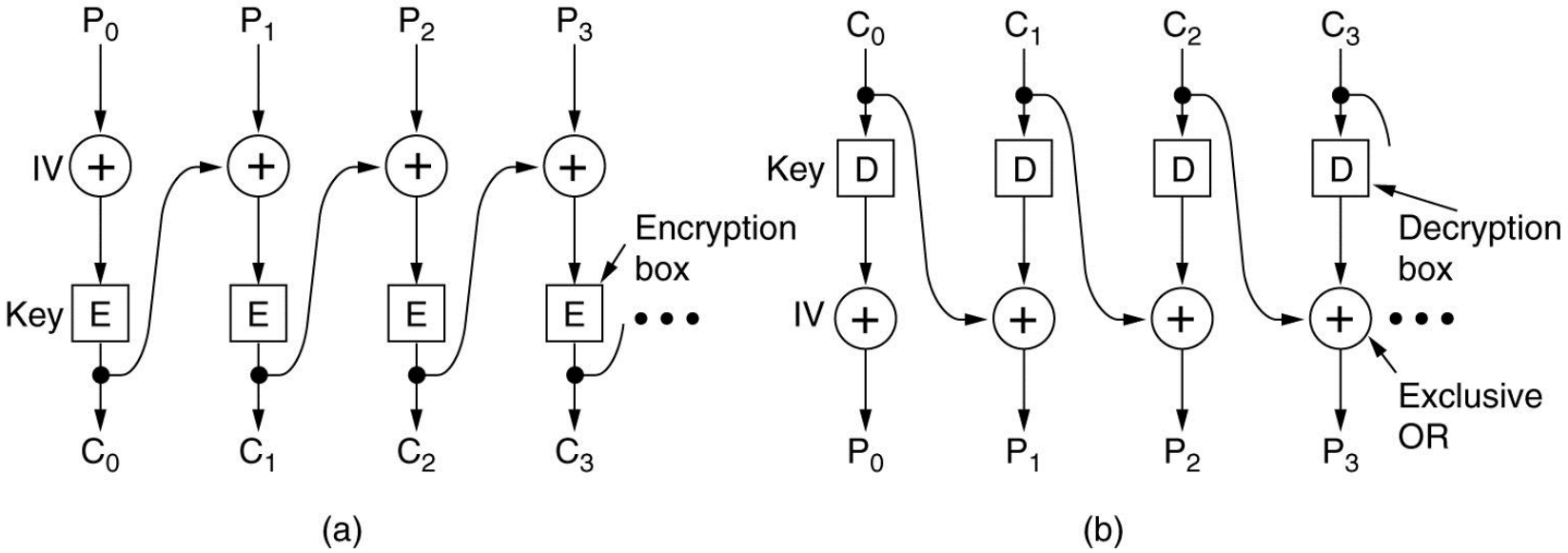
Electronic Code Book Problem



Cipher Block Chaining

- Για να αντιμετωπιστεί το πρόβλημα ECB
- κάθε block γίνεται XOR με το προηγούμενό του πριν κρυπτογραφηθεί.
- Το προηγούμενο έχει ήδη κρυπτογραφηθεί
- Το πρώτο block γίνεται XOR με ένα τυχαίο διάνυσμα αρχικοποίησης IV (initialization vector) που πρέπει να ανταλλαχθεί μαζί με το κλειδί του κώδικα.

Cipher Block Chaining

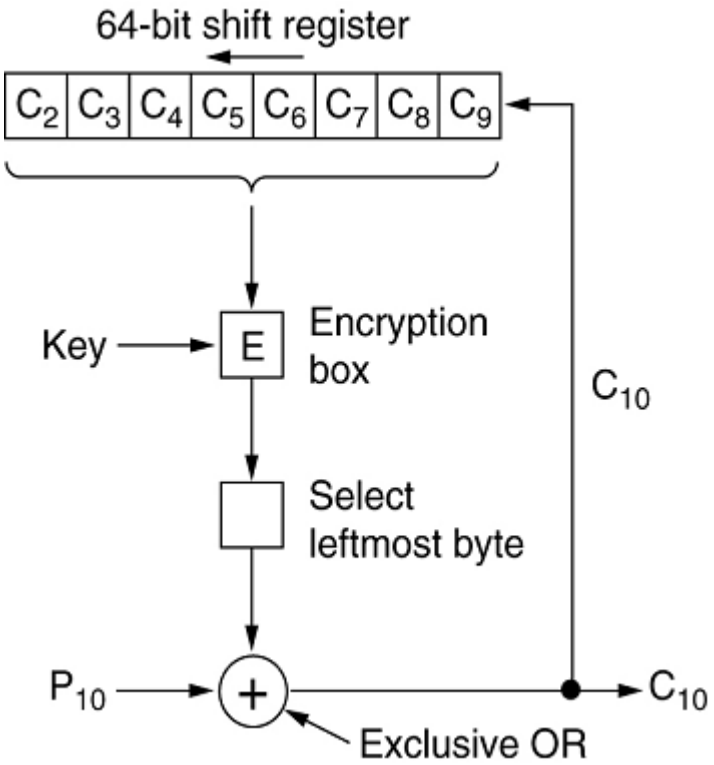


- π.χ. C_0=E(P_0 XOR IV), C_1=E(P_1 XOR IV), ….
  P_0=IV XOR D(C_0)
  κύριο πλεονέκτημα είναι ότι λόγω διαφορετικής αρχικοποίησης το ίδιο κείμενο δεν θα δίνει το ίδιο κρυπτογραφημένο, δυσκολεύοντας έτσι τους κρυπταναλυτές

Cipher Feedback Mode

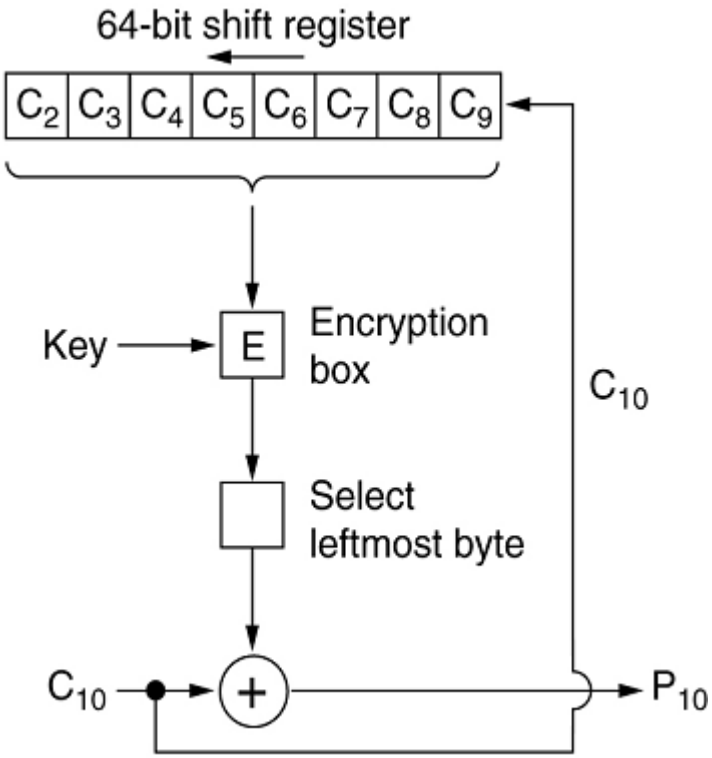
- Ο προηγούμενος τρόπος κωδικοποίησης δεν είναι κατάλληλος όταν θέλω να κωδικοποιήσω μηνύματα με μέγεθος μικρότερο από το block size ή αν δουλεύω με μια διαδραστική εφαρμογή.
- Στην περίπτωση αυτή χρησιμοποιώ *cipher feedback mode* και 3DES. Η περίπτωση του AES είναι ακριβώς ίδια μόνο που οι καταχωρητές ολίσθησης που χρησιμοποιούνται έχουν μέγεθος 128 bit.

Cipher Feedback Mode κρυπτογράφηση



Τα οκτώ προηγούμενα bytes (64 bit) κρυπτογραφούνται και το αριστερότερο byte του αποτελέσματος γίνεται XOR με το προς αποστολή byte. Αντίγραφο αυτού του byte προωθείται στη δεξιότερη θέση του καταχωρητή ολίσθησης.

Cipher Feedback Mode αποκρυπτογράφηση



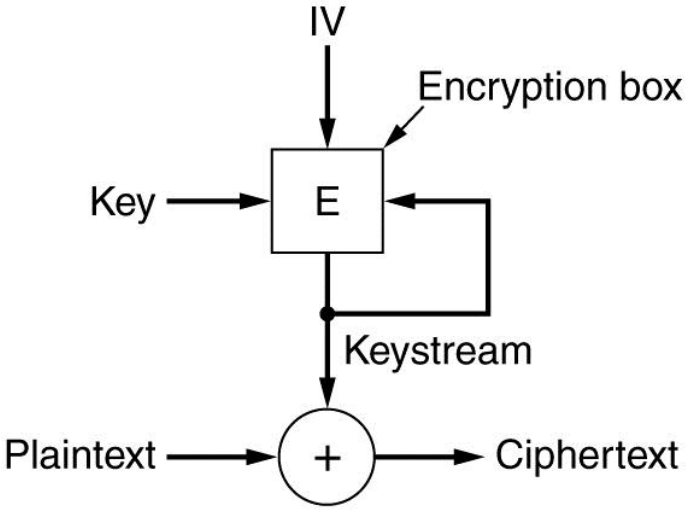
Το κρυπτογραφημένο byte γίνεται XOR με το αριστερότερο byte από την κρυπτογραφημένη έκδοση των προηγούμενων 8 bytes (64 bit) και δίνει το αρχικό Byte.

Ένα πρόβλημα είναι ότι αν καταστραφεί ένα byte τότε θα υπάρξει σφάλμα στην αποκρυπτογράφηση των 8 bytes στα οποία θα συμμετέχει όσο είναι μέσα στον καταχωρητή. Αυτό όμως είναι ένα μικρό τοπικό πρόβλημα.

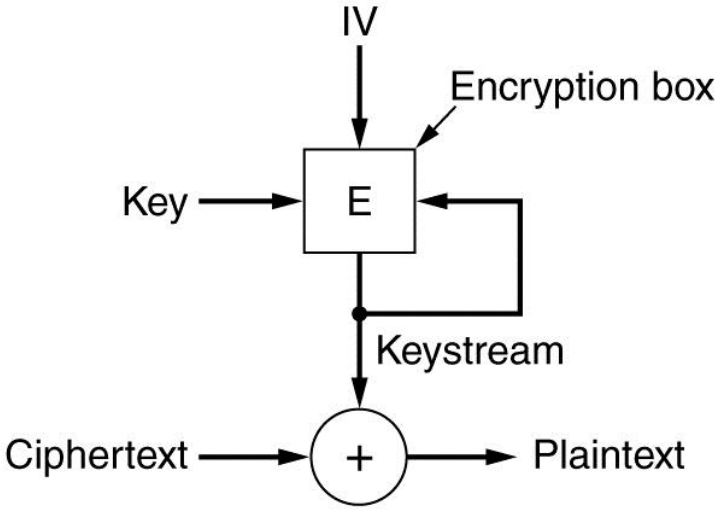
Stream Cipher Mode

- Υπάρχουν εφαρμογές για τις οποίες θεωρείται σοβαρό πρόβλημα το να καταστρέφονται 64 bit λόγω λάθους σε ένα μόνο bit.
- Σε τέτοιες περιπτώσεις μπορεί να εφαρμοστεί μια άλλη τακτική που λέγεται stream cipher mode.
- Ένα διάνυσμα αρχικοποίησης κωδικοποιείται και δίνει μια νέα κωδικοποιημένη ακολουθία (keystream).
- Σε κάθε βήμα η ακολουθία αυτή (που είναι ανεξάρτητη από τα προς κωδικοποίηση δεδομένα) κωδικοποιείται εκ νέου και το αποτέλεσμα γίνεται XOR με το κείμενο προς κρυπτογράφηση.
- Με άλλα λόγια, το keystream χρησιμοποιείται ως ένα one-time-pad.

Stream Cipher Mode



Κρυπτογράφηση σε Stream Mode

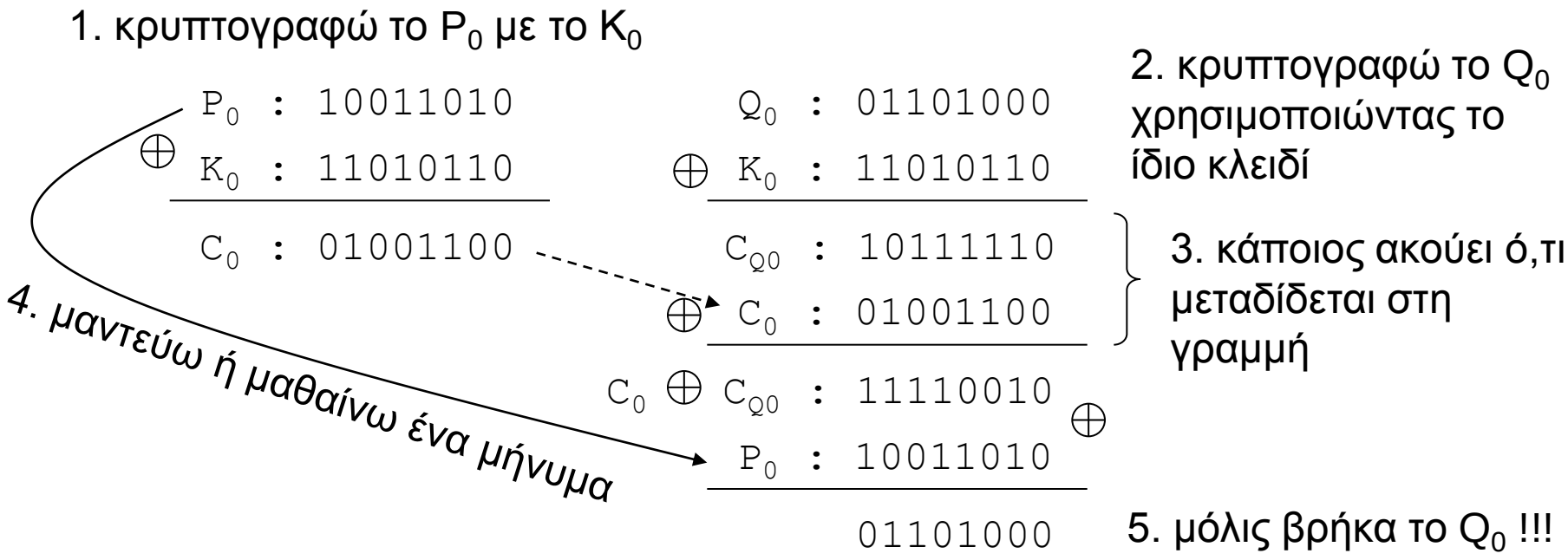


Αποκρυπτογράφηση σε Stream Mode

Το ζεύγος {IV, key} δεν πρέπει να ξανα-χρησιμοποιηθεί.

Αν συμβεί αυτό ο κώδικας είναι εκτεθειμένος σε *"keystream reuse attack"*

Παράδειγμα keystream reuse attack



WEP (γιατί δεν είναι κατάλληλο;)

- **IV:** οι τιμές του μπορούν να ξαναχρησιμοποιηθούν
- **IV: το μήκος τους είναι πολύ μικρό (**24 bit keys που δίνουν περίπου 16.7 εκατομμύρια συνδυασμούς)
- Οι οποίοι ακόμα και σε ένα 11Mbps WiFi μπορούν να εξαντληθούν σε λιγότερο από 5 ώρες (1500*8/(11*10^6)*2^24 = ~18000 seconds)
- **Τα ασθενή κλειδιά είναι ευαίσθητα σε επιθέσεις** (υπάρχουν κλειδιά που θεωρούνται αδύναμα)
- **Τα κύρια κλειδιά (master keys) χρησιμοποιούνται απευθείας!**
- **Η διαχείριση και ανανέωση των κλειδιών γίνεται πολύ δύσκολα, σε σημείο που είναι σαν να μην προσφέρεται.**
- **Ο μηχανισμός ελέγχου της ακεραιότητας μηνυμάτων είναι αναποτελεσματικός**

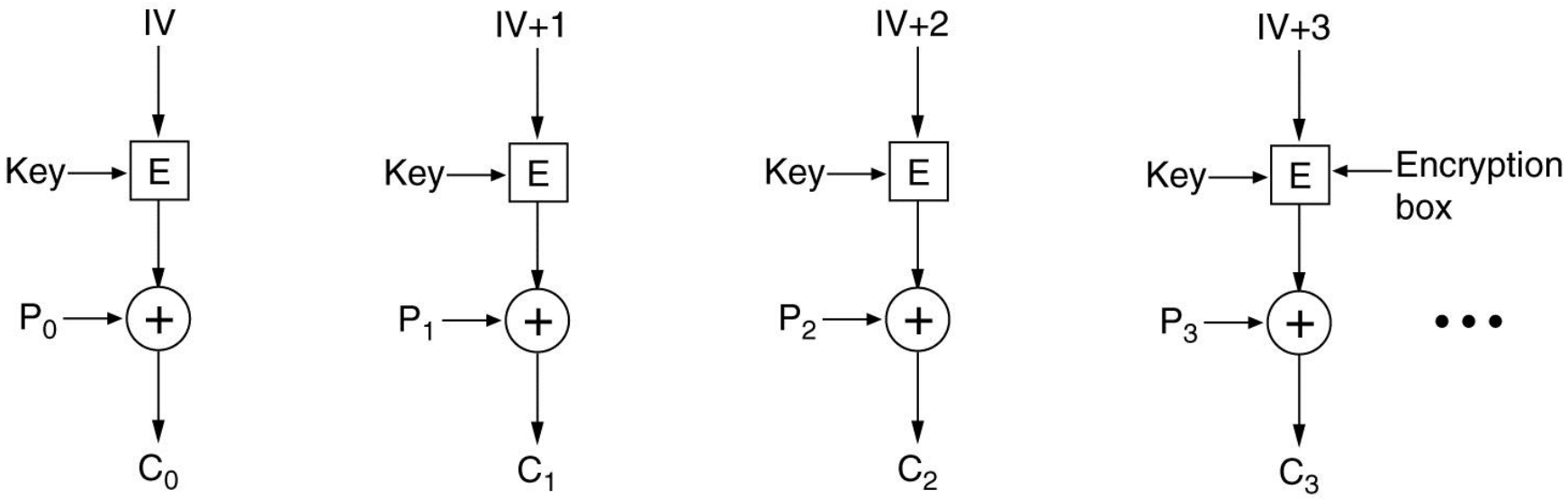
Counter mode

- Το πρόβλημα όλων των παραπάνω τρόπων, εκτός του ECB, είναι ότι για να δω ένα κομμάτι δεδομένων πρέπει να τα αποκρυπτογραφήσω όλα. Αυτό είναι σοβαρό πρόβλημα ειδικά σε περιπτώσεις όπου η πρόσβαση στα δεδομένα γίνεται με μη σειριακό τρόπο, όπως η πρόσβαση στα αρχεία ενός σκληρού δίσκου.
- Για να λυθεί αυτό το πρόβλημα εφευρέθηκε μια μέθοδος κρυπτογράφησης που είναι γνωστή με το όνομα *counter mode*.

Counter mode

- Με τη μέθοδο αυτή το αρχικό κείμενο δεν κρυπτογραφείται άμεσα. Ένα διάνυσμα αρχικοποίησης (IV) κρυπτογραφείται και γίνεται XOR με το πρώτο κομμάτι κειμένου.
- Για κάθε νέο κομμάτι κειμένου το IV αυξάνεται κατά ένα και η διαδικασία επαναλαμβάνεται. Έτσι, κάθε block κειμένου μπορεί να αποκρυπτογραφηθεί ανεξάρτητα από τα υπόλοιπα ανάλογα με τη θέση του.
- Η μέθοδος έχει την ίδια αδυναμία με την προηγούμενη. Είναι ευαίσθητη σε *keystream reuse attack*.

Counter mode



Αλγόριθμοι συμμετρικού κλειδιού

Διανομή κλειδιών

Διανομή κλειδιών

- Η ισχύς κάθε κρυπτογραφικού συστήματος βρίσκεται στη διανομή των κλειδιών.
- Οι δυνατότητες είναι οι εξής:
  1. Ο Α επιλέγει το κλειδί και το δίνει αυτοπροσώπως στον Β
  2. Ένα τρίτο μέρος επιλέγει το κλειδί και το δίνει αυτοπροσώπως στους άλλους δύο
  3. Ο Α και ο Β διαθέτουν ήδη ένα ασφαλές (κρυπτογραφημένο) κανάλι επικοινωνίας και ανταλλάσσουν το κλειδί μέσα από αυτό.
  4. Αν ο Α και ο Β διαθέτουν ήδη ένα ασφαλές κανάλι επικοινωνίας με έναν τρίτο C, ο C μπορεί να παραδώσει το νέο κλειδί στους Α και Β μέσω της σύνδεσης αυτής.

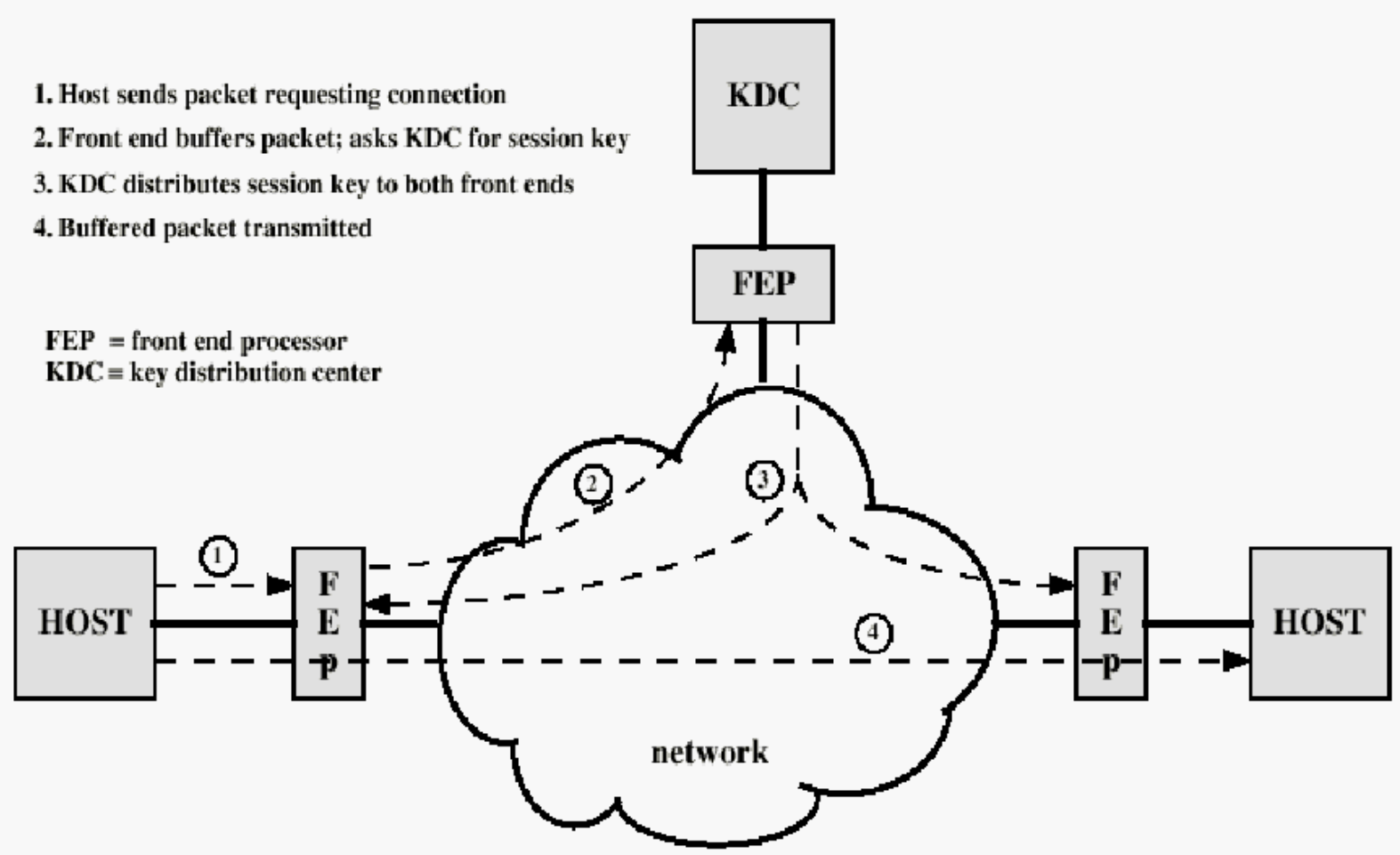
Διανομή κλειδιών

- Προτιμητέα μέθοδος είναι η τέταρτη
- Χρησιμοποιούνται δύο ειδών κλειδιά:
  - Session key: κλειδί μιας χρήσης που χρησιμοποιείται κατά τη διάρκεια μιας επικοινωνίας μεταξύ των μερών.
  - Permanent key: μόνιμο κλειδί γνωστό εκ των προτέρων που δεν ανταλλάσσεται πάνω από το δίκτυο. Χρησιμοποιείται μόνο για την κρυπτογράφηση και αποστολή των session keys.

Στοιχεία υλοποίησης

- Κέντρο διαμοιρασμού κλειδιών (*key distribution center* - KDC): Προσδιορίζει ποιος επιτρέπεται να επικοινωνεί με ποιόν. Όταν δοθεί η εξουσιοδότηση για την επικοινωνία μεταξύ δύο μερών, το KDC παρέχει στους συμμετέχοντες το κλειδί μιας χρήσης (*session key*)
- *Front-end processor*: είναι ο επεξεργαστής που εκτελεί την κρυπτογράφηση από άκρο σε άκρο και παραλαμβάνει τα κλειδιά μιας χρήσης εκ μέρους του Η/Υ ή του τερματικού που εκπροσωπεί.

Αυτόματη διανομή κλειδιού



Τέλος Ενότητας