18/5/2017 -τέλος ύλης

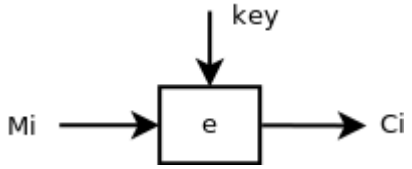
Συμμετρική Κρυπτογραφία

- Για n χρήστες χρειαζόμαστε $\frac{n(n-1)}{2}$ κλειδιά.
- Τα πρωτόκολλα αυτά είναι γρήγορα.
- Τα κλειδιά είναι μικρά σε μέγεθος.

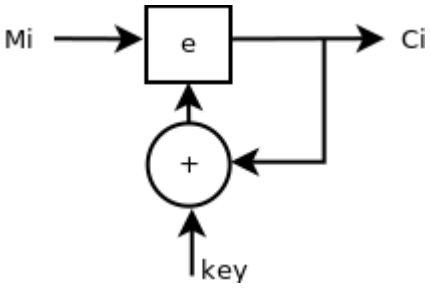
Κατηγορίες Συμμετρικών Πρωτοκόλλων

- Πρωτόκολλα τμήματος (block): κρυπτογραφούν τους χαρακτήρες σε ομάδες.
- Πρωτόκολλα ροής (stream): κρυπτογραφούν ένα χαρακτήρα κάθε φορά. Ουσιαστικά είναι μια ειδική περίπτωση των πρωτοκόλλων τμήματος, με κάθε τμήμα να περιέχει ένα στοιχείο.
- Πρωτόκολλα αντικατάστασης (substitution): ένα από αυτά είναι το πρωτόκολλο του Καίσαρα.
- Πρωτόκολλα αντιμετάθεσης (transposition): αλλάζουν τη σειρά των χαρακτήρων.
- Πρωτόκολλα συνδυασμού (product): είναι συνδυασμός δύο ή περισσότερων από τις παραπάνω κατηγορίες.

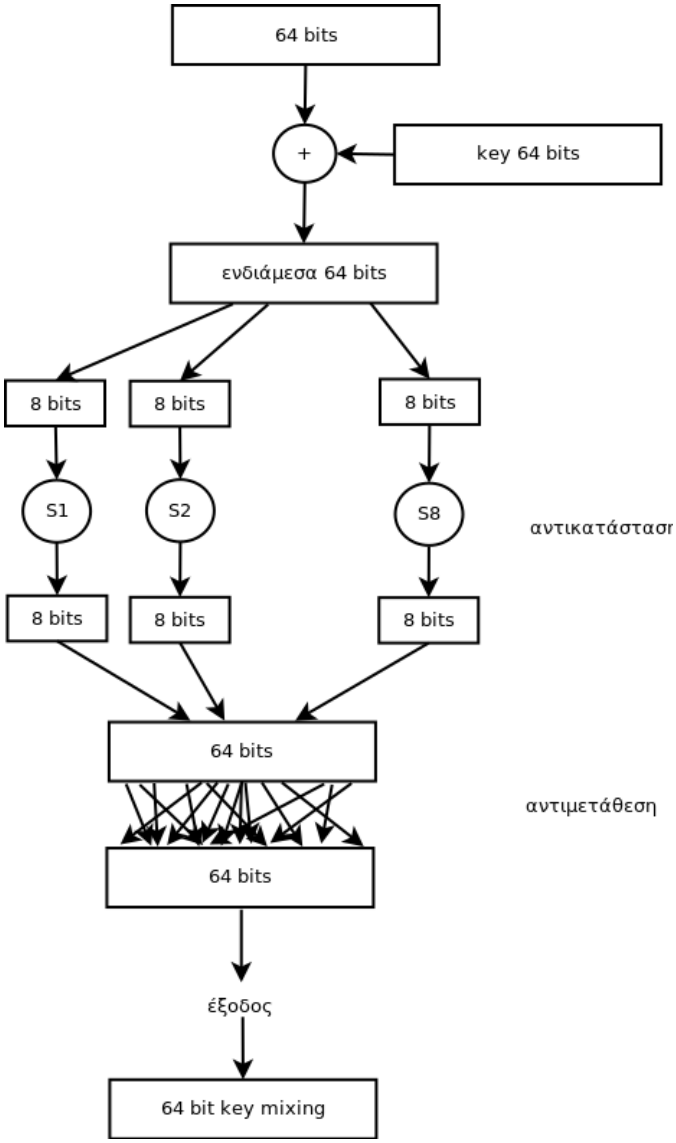
Πρωτόκολλα τμήματος (block)
Έστω ότι έχουμε μέγεθος block 64 bits. Τότε το μήνυμα M_L θα διαιρείται σε t block των 64 bits: $M_L=M_1M_2...M_t$



Με αυτή την προσέγγιση, κάθε φορά που κρυπτογραφούμε ένα $M_ι$ θα παίρνουμε το ίδιο κρυπτογραφημένο μήνυμα C_i. Οπότε αν αλλάξουμε ένα bit, η αλλαγή θα μεταδοθεί μόνο σε ένα bit του κρυπτογραφημένου μηνύματος. Το πρόβλημα αυτό το αντιμετωπίζουμε με την ένθεση ενός αρχικού διανύσματος C_0 το οποίο λέγεται **διάνυσμα αρχικοποίησης (Initialization Vector).**



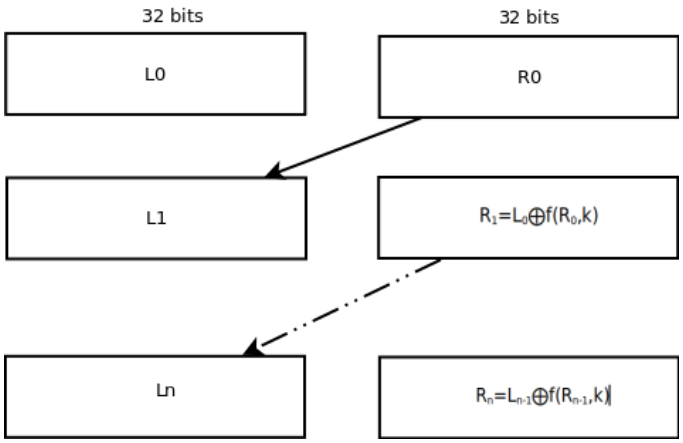
Substitution-Permutation Network



Υποθέτουμε ότι έχουμε εφαρμόσει το σχήμα μια φορά, χωρίς το τελικό βήμα “key mixing”. Η μέθοδος αυτή δεν είναι ασφαλής επειδή μπορούμε να βρούμε το κλειδί ακολουθώντας την αντίστροφη διαδικασία (αφού οι συναρτήσεις αντικατάστασης και αντιμετάθεσης είναι δημόσια γνωστές και όχι απαραίτητα μονόδρομες) και μπορούμε να βρούμε το κλειδί με εξαντλητική αναζήτηση. Η προσθήκη του δεύτερου κλειδιού δεν κάνει το πρωτόκολλο πιο ασφαλές, μιας και μπορούμε να ακολουθήσουμε την ίδια διαδικασία αποκρυπτογράφησης για κάθε εγγραφή του δεύτερου κλειδιού.

Δίκτυο Feistel

Το χαρακτηριστικό αυτού του δικτύου είναι ότι τα ενδιάμεσα συστατικά δεν είναι αντιστρέψιμα, αλλά το τελικό αποτέλεσμα είναι.



Οι συναρτήσεις αντικατάστασης και αντιμετάθεσης δεν είναι τυχαίες, αλλά επιλέγονται ώστε για ΜΜ' που διαφέρουν σε 1 bit, παίρνουμε CC' που διαφέρουν παντού, εφόσον έχουμε πολλές επαναλήψεις του αλγορίθμου.

DES-Data Encryption Standard

Είναι ένα δίκτυο τύπου Feistel, με 16 γύρους, μέγεθος block 64 bits και μέγεθος κλειδιού 56 bits το οποίο γεννά 48 κλειδιά. Το δίκτυο αυτό δεν έσπασε ποτέ, αλλά αποσύρθηκε επειδή πλέον είναι εύκολο να βρούμε όλα τα κλειδιά με εξαντλητική αναζήτηση. Δεν μπορούμε να αυξήσουμε το μήκος του κλειδιού επειδή τότε θα χάσουμε τις ιδιότητες που κάνουν το δίκτυο άθραυστο. Χρησιμοποιείται όμως η παραλλαγή του που λέγεται Triple DES.

Γύρος j: $f(R_0, k_j)$

$R_j=L_{j-1} \oplus f(R_{j-1},k_j)$

$f(R_{j-1},k_j)=P(S(E(R_{j-1})+K_j))$

όπου οι συναρτήσεις P, S, E είναι:

E: επέκταση από 32 σε 48 bits.

S: αντικατάσταση 48 bits με 8 S-boxes. Σε κάθε S-box τα 6 bit γίνονται 4, άρα επιστρέφουμε στα 32 bits.

P: αντιμετάθεση 32 bits.