Κρυπτογραφία

Κρυπτοσυστήματα τμήματος (Block ciphers)

Άρης Παγουρτζής – Στάθης Ζάχος – Πέτρος Ποτίκας

Εθνικό Μετσόβιο Πολυτεχνείο
Σχολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών

Block ciphers (κρυπτοσυστήματα τμήματος)

- Block cipher = αποδοτική, με κλειδί, ψευδοτυχαία μετάθεση $F : \{0,1\}^n \times \{0,1\}^l \mapsto \{0,1\}^l$
- $F_k(x) = F(k,x)$ είναι μια ένα-προς-ένα και επί συνάρτηση (δηλ. μετάθεση) και F_k, F_k^{-1} αποδοτικά υπολογίσιμες για δοσμένο k
- $n =$ μήκος κλειδίου
  $l =$ μήκος block
- Τα n, l είναι παράμετροι (μας ενδιαφέρει 'συγκεκριμένη' ασφάλεια, όχι ασυμπτωτική!)
- Θέλουμε ο αντίπαλος να μπορεί να σπάσει το σύστημα μόνο με (σχεδόν) εξαντλητική αναζήτηση κλειδιού

Δίκτυα Feistel

Δίκτυα Feistel [H. Feistel 1973]

- Blowfish, Lucifer, DES, IDEA, RC5, SMS4, RC6, …
- Κρυπτοσυστήματα τμήματος (block cryptosystems): το αρχικό κείμενο χωρίζεται σε block συγκεκριμένου μήκους (π.χ. για DES: 64 bits).
- Στο εξής θα ασχοληθούμε με την κρυπτογράφηση ενός μόνο τμήματος (block):
  - Είσοδος: $L_0||R_0$
  - Σε κάθε γύρο i, για $i = 1, 2, ..., r$:
    $L_i = R_{i-1}$
    $R_i = F(R_{i-1}, K_i) \oplus L_{i-1}$
  - Έξοδος: $R_r||L_r$.
  - k_i: το κλειδί του γύρου i – παράγεται από το αρχικό κλειδί, συνήθως με ολισθήσεις.
  - F: συνάρτηση που είναι η "καρδιά" του συστήματος: πρέπει να προκαλεί σύγχυση (confusion) και διάχυση (diffusion) — Shannon ξανά!.

Δίκτυα Feistel

Σημαντικές ιδιότητες των δικτύων Feistel

Η αποκρυπτογράφηση γίνεται με τον ίδιο τρόπο, απλά αντιστρέφοντας τη σειρά των κλειδιών.

Επομένως, η συνάρτηση F δεν χρειάζεται να είναι αντιστρεπτή, σε αντίθεση με τα *Subsitution-Permutation networks*.

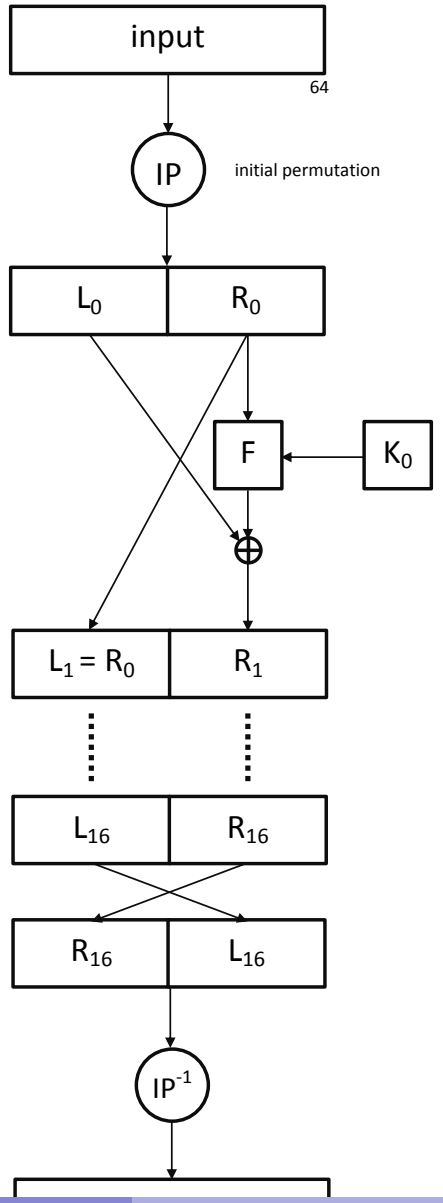
Το κρυπτοσύστημα DES

Δίκτυο Feistel 16 γύρων.

Μήκος block: 64 bits.

Μήκος κλειδιού: 64 bits (56 ‘ενεργά’ + 8 ισοτιμίας).

IP: αρχική μετάθεση (initial permutation).



Το κρυπτοσύστημα DES

Η συνάρτηση F

- Συστατικά: συνάρτηση επέκτασης E, συναρτήσεις ("κουτιά") αντικατάστασης S (S-boxes), μετάθεση P.
  - $E : \{0,1\}^{32} \mapsto \{0,1\}^{48}$
  - $S_i : \{0,1\}^{6} \mapsto \{0,1\}^{4}, \quad 0 \leq i \leq 7$
  - $P : \{0,1\}^{32} \mapsto \{0,1\}^{32}$.
- Η E παίρνει κάθε 4-άδα bits της εισόδου της και τα συμπληρώνει με τα διπλανά της: π.χ. $b_0 b_1 b_2 b_3 \xrightarrow{E} b_{31} b_0 b_1 b_2 b_3 b_4$, δίνοντας σαν αποτέλεσμα οκτώ 6-άδες.
- Το αποτέλεσμα της E γίνεται XOR με το κλειδί γύρου K_i (48 bits).
- Κάθε 6-άδα του αποτελέσματος αντικαθίσταται μέσω του αντίστοιχου S-box από μία 4-άδα.
- Η εφαρμογή της P δίνει το τελικό αποτέλεσμα.

Το κρυπτοσύστημα DES

S-boxes

S_1															
14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

Είναι πίνακες 4×16.

Κάθε 6-άδα απεικονίζεται σε μία θέση του πίνακα ως εξής: το 1ο και το 6ο ψηφίο $(b_0 b_5)$ καθορίζουν τη σειρά, τα ψηφία 2ο-5ο $(b_1 b_2 b_3 b_4)$ τη στήλη.

Στην κάθε θέση βρίσκεται ένας αριθμός από 0 έως 15, δηλ. μια 4-άδα bits, που είναι η έξοδος του S-box για είσοδο $b_0 b_1 b_2 b_3 b_4 b_5$.

Το κρυπτοσύστημα DES

Ιδιότητες των S-boxes (i)

- Είναι το μη γραμμικό συστατικό του DES, και γι'αυτό το πιο σημαντικό: χωρίς αυτό η κρυπτανάλυση θα ήταν εύκολη.
- Ειδικά σχεδιασμένα ώστε να προκαλούν σύγχυση (confusion): η σχέση ενός bit του κλειδιού και ενός bit εξόδου είναι πολύπλοκη. Κάθε bit της εξόδου επηρεάζεται από πολλά bits του κλειδιού.
- Η διάχυση (diffusion) εξασφαλίζεται σε συνδυασμό με τις συναρτήσεις επέκτασης E και μετάθεσης P: κάθε bit της εισόδου επηρεάζει πολλά bits της εξόδου.

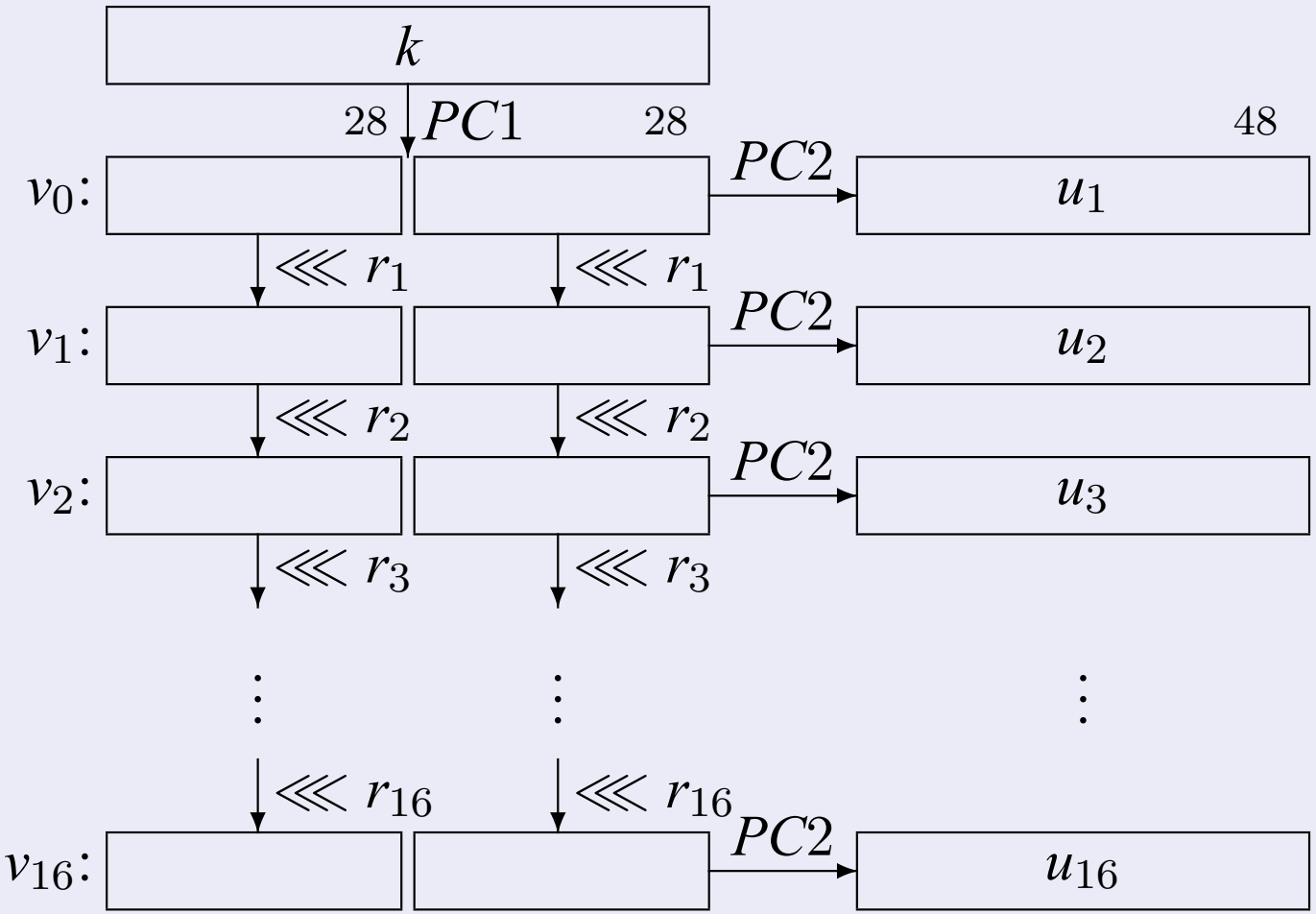
Το κρυπτοσύστημα DES

Ιδιότητες των S-boxes: NSA design criteria

- Κάθε σειρά είναι μετάθεση του $\{0, \ldots, 15\}$.
- Κανένα S-box δεν είναι γραμμική ή αφφινική συνάρτηση των εισόδων του.
- Αλλαγή ενός bit εισόδου επιφέρει αλλαγή σε τουλάχιστον δύο bit εξόδου.
- Για οποιοδήποτε ζεύγος bit εισόδου και bit εξόδου, αν καθορίσουμε την τιμή του bit εισόδου το πλήθος εισόδων που κάνουν το bit εξόδου '0' είναι περίπου ίδιο με το πλήθος εισόδων που κάνουν το bit εξόδου '1'.

Το κρυπτοσύστημα DES

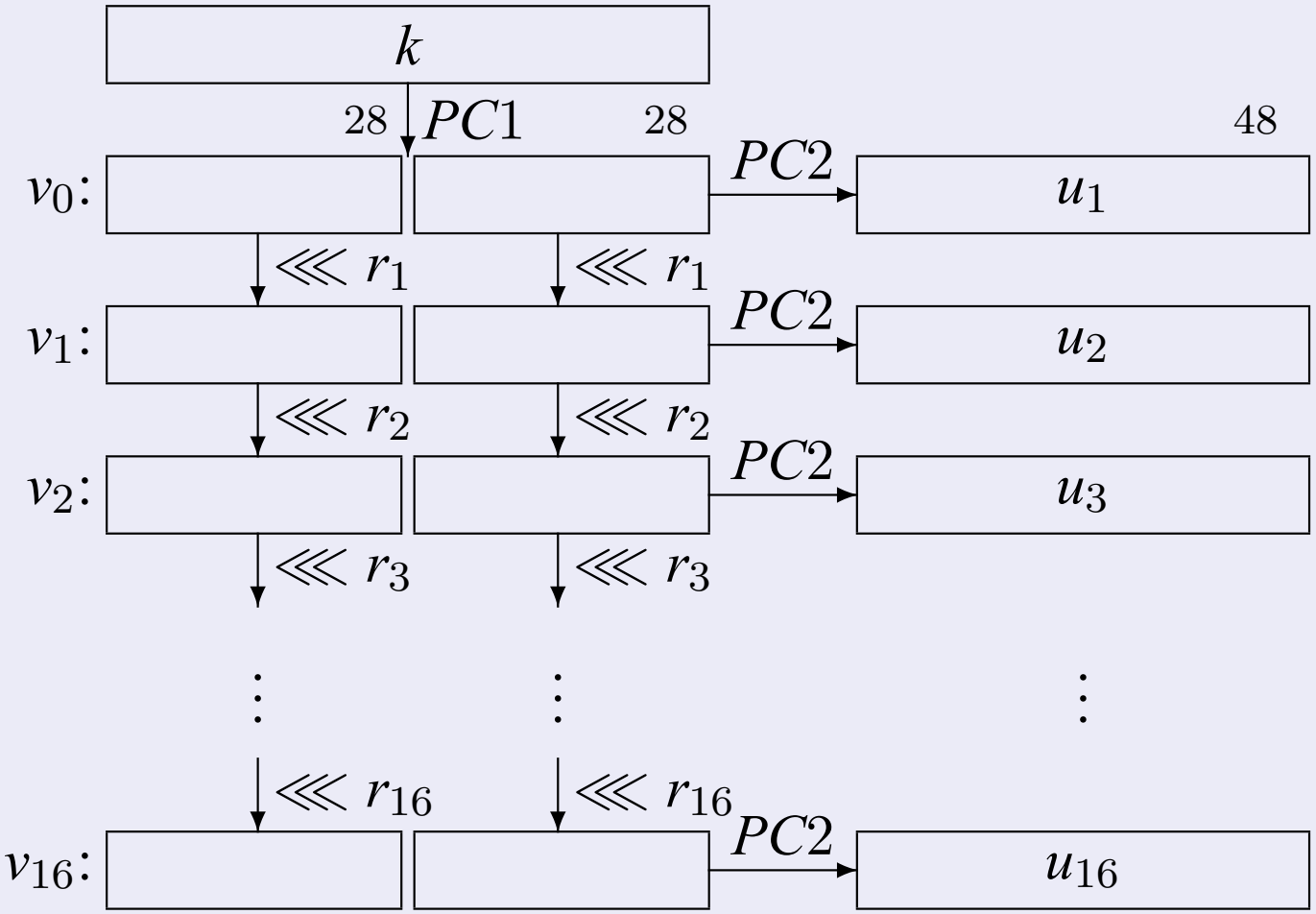
Η παραγωγή των κλειδιών



Βασίζεται σε διαδοχικές ολισθήσεις των 56 ενεργών bits του κλειδιού, και σε συναρτήσεις επιλογής $\{0,1\}^{56} \mapsto \{0,1\}^{48}$.

Το κρυπτοσύστημα DES

Η παραγωγή των κλειδιών



i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
r_i	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1
συν.	1	2	4	6	8	10	12	14	15	17	19	21	23	25	27	28

Το κρυπτοσύστημα DES

Ιδιότητες του 'προγράμματος' παραγωγής κλειδιών

- Κάθε bit του κλειδιού χρησιμοποιείται ως είσοδος σε κάθε S-box (σε κάποιο γύρο).
- Κανένα bit του κλειδιού δεν χρησιμοποιείται ως είσοδος στο ίδιο S-box σε διαδοχικούς γύρους.
- Στο τέλος έχει γίνει μία πλήρης περιστροφή, επιτρέποντας στην αποκρυπτογράφηση να γίνει με ολισθήσεις προς τα δεξιά (κατά αντίστροφη σειρά).

Το κρυπτοσύστημα DES: επιθέσεις

- Brute force: 2^{56} δοκιμές.
- Complementarity property: $E(K, M) = C \Leftrightarrow E(\bar{K}, \bar{M}) = \bar{C}$
  Επιτρέπει κρυπτανάλυση με 2^{55} δοκιμές (*άσκηση*: πώς;).
- Διαφορική κρυπτανάλυση (differential cryptanalysis) [Shamir, Biham, 1990, NSA και IBM, νωρίτερα]: $< 2^{50}$ δοκιμές με *επιλεγμένα κρυπτοκείμενα* (CPA). Βασίζεται στους πίνακες κατανομής των διαφορών εισόδου (input-XOR) και εξόδου (output-XOR) των S-boxes. Η μη ομοιομορφία στις κατανομές επιτρέπει περιορισμό του συνόλου των πιθανών κλειδιών.
- Γραμμική κρυπτανάλυση (linear cryptanalysis) [Matsui, 1993]: 2^{43} δοκιμές με *γνωστά κρυπτοκείμενα* (KPA). Προσέγγιση της λειτουργίας των S-boxes με γραμμικές συναρτήσεις των εισόδων τους. Ενδεχόμενη πόλωση μπορεί να αποκαλύψει πληροφορίες για το κλειδί.
- Στα τέλη του '90 θεωρήθηκε μη ασφαλές (EFF DES cracker, 1998) και το NIST πρότεινε την αντικατάστασή του: ανάπτυξη και υιοθέτηση του AES.

Το κρυπτοσύστημα DES: άμυνες

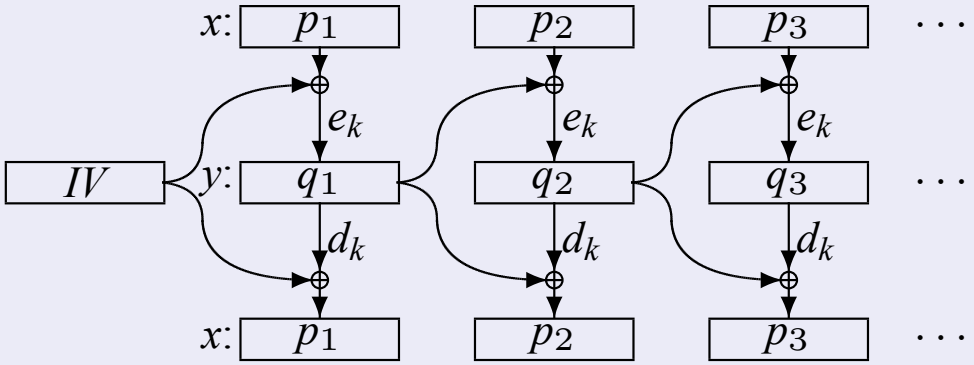
- Μια πρώτη προσπάθεια: Double DES. Πρόβλημα: meet-in-the middle (MITM) attack.
- Triple DES (3-DES): effective key 118 bits (με 3 ανεξάρτητα κλειδιά, συνολικό μήκος κλειδιού 168 bits) ή 112 bits (με 2 ανεξάρτητα κλειδιά, συνολικό μήκος 112 bits). Χρησιμοποιείται ακόμη και σήμερα (εκτίμηση ασφάλειας από NIST: $\sim$ 2030).
  Κρυπτογράφηση: $Enc_{3-\mathrm{DES}}(x) = E_{k_1}(D_{k_2}(E_{k_3}(x))))$ (backwards compatibility με απλό DES).
- DES-X: μήκος κλειδιού 184 bits, effective key $\sim$ 119 bits.
  Κρυπτογράφηση: $Enc_{\mathrm{DES-X}}(x) = k_2 \oplus E_{k_3}(x \oplus k_1)$

Τρόποι λειτουργίας του DES (operation modes)

(και άλλων κρυπτοσυστημάτων τμήματος)

ECB, CBC: το block cipher ενεργεί στο plaintext (άμεσα ή έμμεσα)

- Electronic Code Book (ECB): κάθε τμήμα κρυπτογραφείται χωριστά.
- Cipher Block Chaining (CBC): το κρυπτογράφημα του προηγούμενου τμήματος κρυπτοκειμένου γίνεται XOR με το τρέχον τμήμα αρχικού κειμένου πριν αυτό κρυπτογραφηθεί. Χρησιμοποιείται Initial Vector (IV) για το πρώτο τμήμα.



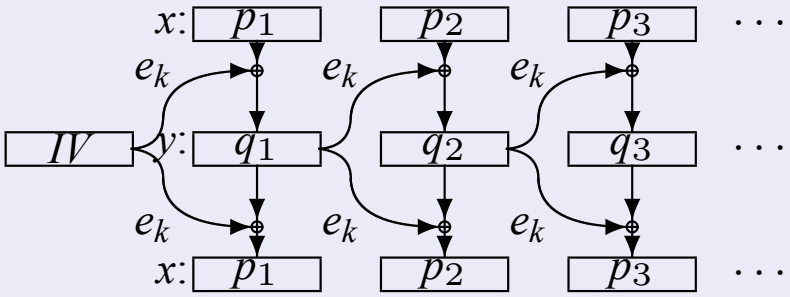
CBC mode

Τρόποι λειτουργίας του DES (operation modes)

(και άλλων κρυπτοσυστημάτων τμήματος)

CFB, OFB, CTR: δημιουργία κλειδοροής (⇒ stream cipher)

Cipher Feedback mode (CFB): δημιουργεί τμηματική κλειδοροή (keystream) που χρησιμοποιείται όπως σε stream cipher. Το κλειδί που γίνεται XOR με το τρέχον τμήμα αρχικού κειμένου προκύπτει από κρυπτογράφηση του προηγούμενου τμήματος κρυπτοκειμένου – χρησιμοποιείται IV για το πρώτο τμήμα.



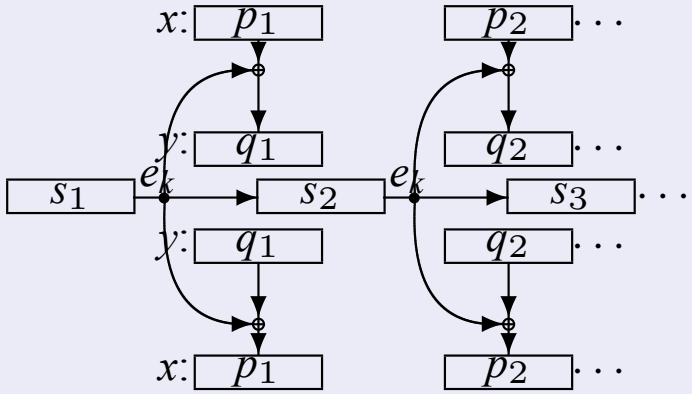
CFB mode

Τρόποι λειτουργίας του DES (operation modes)

(και άλλων κρυπτοσυστημάτων τμήματος)

CFB, OFB, CTR: δημιουργία κλειδοροής (⇒ stream cipher)

Output Feedback mode (OFB): δημιουργεί keystream όπως το CFB. Το κλειδί που γίνεται XOR με το τρέχον τμήμα αρχικού κειμένου προκύπτει από κρυπτογράφηση του προηγούμενου κλειδιού – χρησιμοποιείται IV για το πρώτο τμήμα.



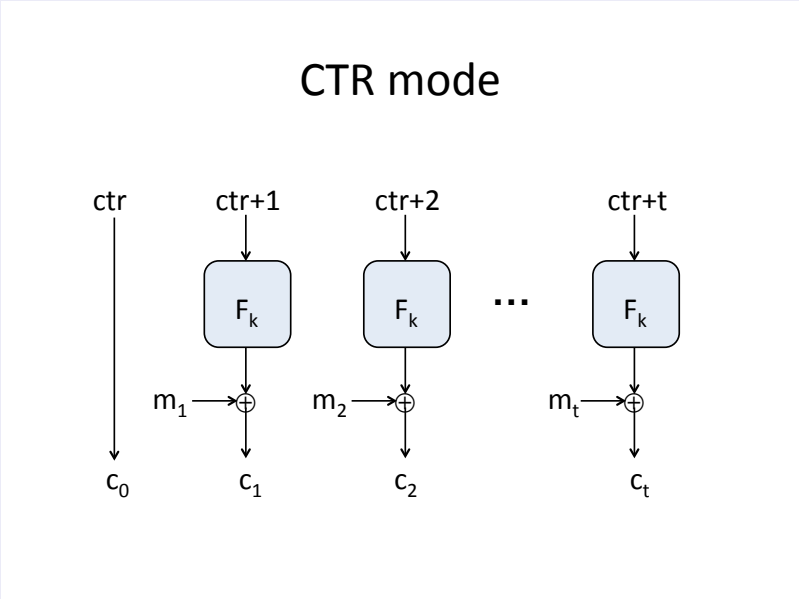
OFB mode

Τρόποι λειτουργίας του DES (operation modes)

(και άλλων κρυπτοσυστημάτων τμήματος)

CFB, OFB, CTR: δημιουργία κλειδοροής (⇒ stream cipher)

Counter mode (CTR): δημιουργεί keystream όπως και τα CFB, OFB. Η διαφορά έγκειται στο ότι το κλειδί για το τρέχον τμήμα προκύπτει από την κρυπτογράφηση ενός μετρητή, που αυξάνεται από τμήμα σε τμήμα. Χρήση με nonce.

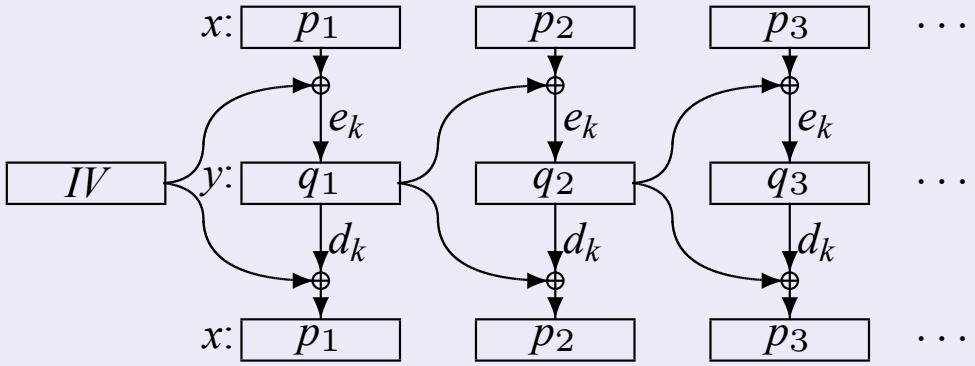


Τρόποι λειτουργίας του DES (operation modes)

ECB, CBC: πλεονεκτήματα και αδυναμίες

- ECB (-): κάθε τμήμα κρυπτογραφείται με τον ίδιο τρόπο. Εντοπισμός επαναλήψεων, στατιστικές επιθέσεις.
  ECB (+): σε περίπτωση αλλοίωσης τμήματος κρυπτοκειμένου δεν επηρεάζεται η αποκρυπτογράφηση των υπολοίπων τμημάτων.

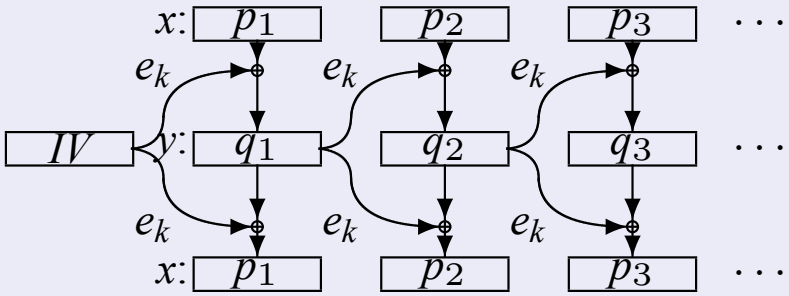
  CBC (-): Με αλλοιώσεις bit του κρυπτοτμήματος y_i προκύπτει αλλοίωση του αποτελέσματος x_{i+1} στις ίδιες θέσεις.
  CBC (+): χρήση ως Message Authentication Code (MAC).
  Authenticated encryption. Σε περίπτωση αλλοίωσης τμήματος κρυπτοκειμένου επηρεάζονται μόνο δύο τμήματα στην αποκρυπτογράφηση: Self-Recovery. Το IV δεν είναι κρυφό.



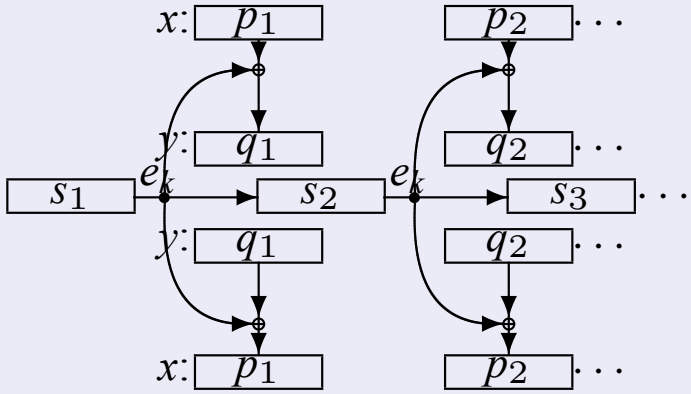
CBC mode

Τρόποι λειτουργίας του DES (operation modes)

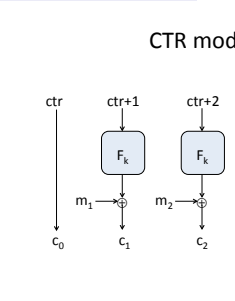
CFB, OFB, CTR: πλεονεκτήματα και αδυναμίες



CFB mode



OFB mode



- CFB / OFB / CTR (-): σε όλα υπάρχει το πρόβλημα της αλλοίωσης της αποκρυπτογράφησης σε επιλεγμένες θέσεις.
- CFB / OFB / CTR (+): Μπορούν να υλοποιηθούν παράλληλα. Διαθέτουν self-recovery.
- CFB (+): μπορεί να χρησιμοποιηθεί ως MAC. **Άσκηση**: μπορούμε να έχουμε encryption και authentication σε ένα πέρασμα;
- CFB / OFB (+): χρήση και για block μικρότερα των 64 bit.

Και άλλοι πολλοί τρόποι λειτουργίας

- Για κρυπτογράφηση.
- Για αυθεντικοποίηση / ακεραιότητα.
- Και για τα δύο (authenticated encryption).
- Δείτε τη σχετική σελίδα του NIST: http://csrc.nist.gov/groups/ST/toolkit/BCM/modes_development.html

AES

- Το 1997 το NIST (National Institute of Standards and Technology) ανακοίνωσε διαγωνισμό για την αντικάτασταση του DES
- 15 αλγόριθμοι προτάθηκαν από ομάδες από όλον τον κόσμο
- Οι προτάσεις εξετάστηκαν από μέλη του NIST, από άλλους κρυπτογράφους αλλά και κυρίως τις ίδιες τις ομάδες
- Δύο συνέδρια έγιναν το 1998 και 1999 για να αποφασιστεί ο καλύτερος
- Το 2000 αποφασίστηκε ο αλγόριθμος Rijndael (John Daemen, Vincent Rijmen - Belgium)
- Οι 5 φιναλίστ πληρούσαν το κριτήριο της ασφάλειας και ο νικητής κρίθηκε από την αποδοτικότητα, ευελιξία, ευκολία υλοποίησης κλπ.

AES

- Block cipher με μήκος block 128 bits
- Μήκος κλειδιού 128, 192, 256 bits
- Σε αντίθεση με το DES που είναι ένα δίκτυο Feistel, το AES είναι ένα δίκτυο αντικατάστασης-μετάθεσης
- Ένας 4×4 πίνακας από bytes, που λέγεται state, τροποποιείται σε κάθε γύρο
- Αρχικά το state αποτελείται από την είσοδο (128 bits = 16 bytes)
- 10, 12, 14 γύροι, για κλειδί 128, 192, 256 αντίστοιχα
- Στον τελευταίο γύρο το MixColumns αντικαθίσταται με ένα AddRoundKey (αποτροπή αντιστροφής των τελευταίων 3 σταδίων, που δεν εξαρτώνται από το κλειδί)

AES

Τα παρακάτω τέσσερα στάδια εφαρμόζονται σε κάθε γύρο:

- *Στάδιο 1*-AddRoundKey: από το master key, παράγεται ένα 128-bit υποκλειδί, και το βλέπουμε σαν 4×4 πίνακα από bytes. Ο πίνακας state ενημερώνεται με το XOR της τρέχουσας τιμής και του υποκλειδιού.
- *Στάδιο 2*-SubBytes: κάθε byte του state αντικαθίσταται από ένα άλλο, με βάση ένα κουτί αντικατάστασης (S-box). Αυτός ο πίνακας είναι μια ένα-προς-ένα και επί συνάρτηση στο $\{0,1\}^8$. Υπάρχει μόνο ένα S-box, και κάθε byte του state αλλάζει.
- *Στάδιο 3*-ShiftRows: τα bytes κάθε γραμμής του state ολισθαίνουν κυκλικά προς τα αριστερά ως εξής: η πρώτη γραμμή δεν αλλάζει, η δεύτερη ολισθαίνει κατά μία θέση, η τρίτη κατά δύο, η τέταρτη κατά τρεις θέσεις.
- *Στάδιο 4*-MixColumns: ένας αντιστρέψιμος μετασχηματισμός εφαρμόζεται σε κάθε στήλη. Πολλαπλασιασμός κάθε στήλης με ένα κατάλληλο vector.

Τα στάδια 1, 2 προκαλούν σύγχυση, ενώ τα 3, 4 διάχυση.

Ασφάλεια του AES

- Γνωστές επιθέσεις:
  1. 6-γύρων AES με 128-bits κλειδί, με κρυπτογραφήσεις τάξης 2^{72}
  2. 8-γύρων AES με 192-bits κλειδί, με κρυπτογραφήσεις τάξης 2^{188}
  3. 8-γύρων AES με 256-bits κλειδί, με κρυπτογραφήσεις τάξης 2^{204}
- Επιθέσεις σε AES περιορισμένων γύρων, ενώ σε πλήρες AES μέχρι σήμερα το καλύτερο που έχουμε είναι επιθέσεις εξαντλητικής αναζήτησης του κλειδιού
- Εξαιρετικό για κρυπτογραφία που χρειάζεται ψευδοτυχαίες μεταθέσεις
- Είναι ελεύθερο, αποδοτικό, προτυποποιήμενο και εξαιρετικά ασφαλές

Block ciphers: σύνοψη

- Τα δύο πρότυπα: DES (παλαιότερα) και AES (τώρα)
- Έλλειψη αυστηρών εγγυήσεων ασφάλειας
- Ισχυρές ευριστικές μέθοδοι, αντοχή σε πλήθος επιθέσεων
- Η ασφάλειά τους βασίζεται σε ιδιότητες που άντεξαν στο 'τεστ του χρόνου'
- Χρήση και σε κρυπτοσυστήματα ροής (CFB, OFB, CTR modes)