Κρυπτογραφία

Καραγκούνης Λεωνίδας

Παράδοξο Γενεθλίων

Δοκιμές με πιθανότητα $p(n)$ να βρούμε δύο ίσους αριθμούς σε πλήθος m:
$r \approx \sqrt{2m \cdot p(n)}$
Για πιθανότητα 50% έχουμε $r \approx \sqrt{2m \cdot \frac{1}{2}} = \sqrt{m}$

Χρήσιμες πληροφορίες

DECIMAL	BINARY	HEXADECIMAL	OCTAL
0	0000	0	0
1	0001	1	1
2	0010	2	2
3	0011	3	3
4	0100	4	4
5	0101	5	5
6	0110	6	6
7	0111	7	7
8	1000	8	10
9	1001	9	11
10	1010	A	12
11	1011	B	13
12	1100	C	14
13	1101	D	15
14	1110	E	16
15	1111	F	17

Κρυπτογραφία συμμετρικού κλειδιού

Σε ένα δίκτυο με n κόμβους, για την ανά δύο ασφαλή επικοινωνία τους, χρειάζονται συνολικά $n(n-1)/2$ συμμετρικά κλειδιά συνόδου.
Αλλαγή κλειδιού για κάθε νέα σύνοδο και συμμετοχή Trusted Third Party για αποδοτική διαχείριση κλειδιών.

ECB & CBC

ECB Χωρισμός σε δέσμες 64 bit, κρυπτογράφηση κάθε δέσμης με DES.
Ενδείκνειται για μικρές δέσμες όπως κρυπτογράφηση κλειδιών DES. Αδυναμία σε μεγάλες δέσμες καθώς:
Ίδιες δέσμες εισόδου $\rightsquigarrow$ Ίδια κρυπτογραφήματα.
Ένα λάθος του ενός bit στο κρυπτογραφημένο κείμενο θα προκαλέσει αλλοίωση μιας δέσμης αρχικού κειμένου ($n/2$ bits με λάθη κατά μέσο όρο).

CBC

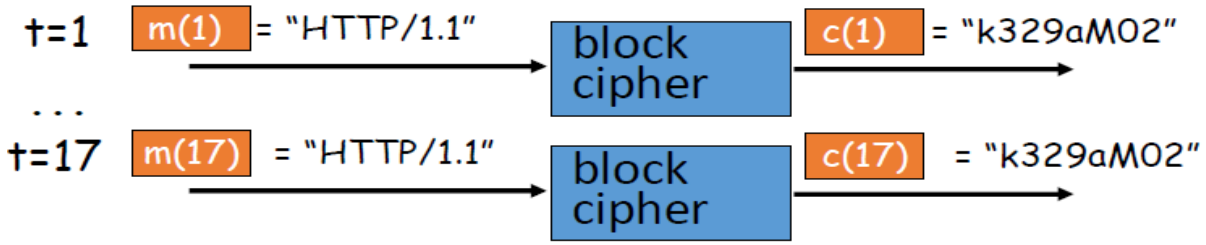
Προηγούμενη είσοδο $m(i)$ **XOR** προηγούμενη κρυπτογραφημένη δέσμη $c(i-1)$.

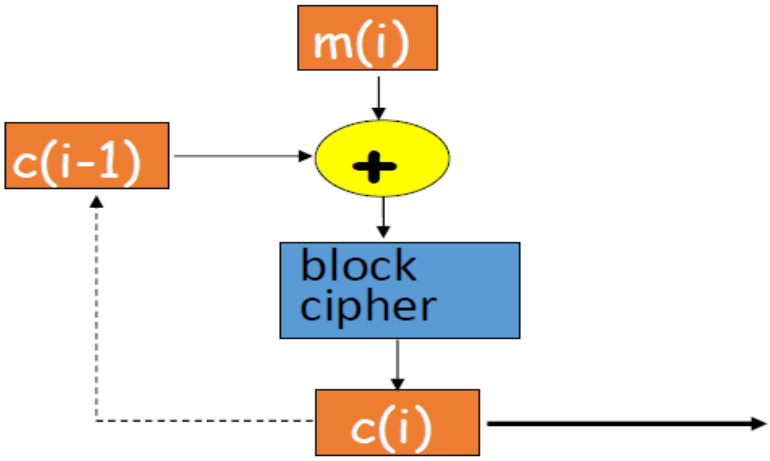
Κρυπτογραφημένη δέσμη $c(i) = m(i) \oplus c(i-1)$

Η αρχική είσοδο m(0) κρυπτογραφείται με μια τυχαία τιμή αρχικοποίησης (ή παράγεται με κάποια συμφωνημένη διαδικασία) SV, η οποία ανταλλάσεται μαζί με το κλειδί κατά την αρχική επικοινωνία.

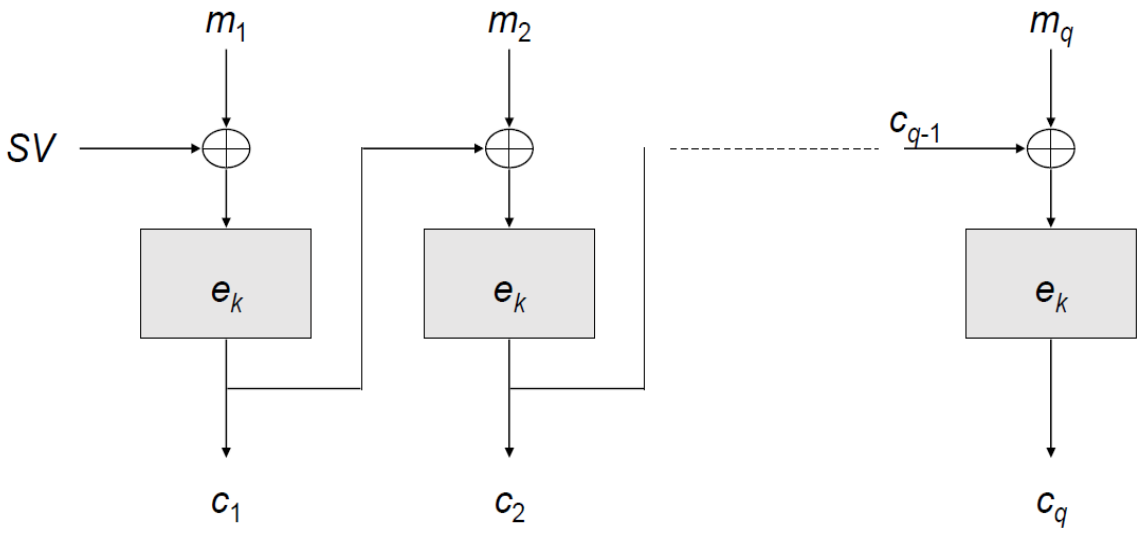
Κατάλληλος για κρυπτογράφηση μηνυμάτων μεγαλύτερων από 64 bit.

Ένα λάθος του ενός bit στο κρυπτογραφημένο κείμενο θα προκαλέσει αλλοίωση μιας δέσμης αρχικού κειμένου και ενός λανθασμένου bit στη δέσμη που ακολουθεί ($n/2 + 1$ bits με λάθη κατά μέσο όρο).





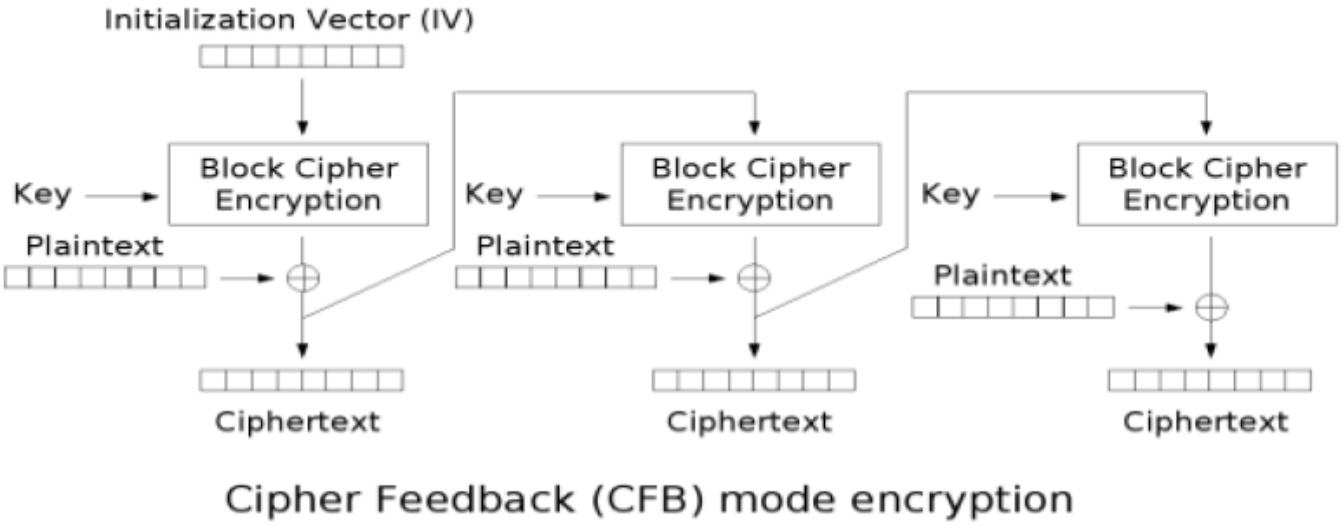
Κρυπτογράφηση ECB & CBC (ΕΑΠ ΠΛΗ35 - 3η ΟΣΣ Γιάννης Μαυρίδης)

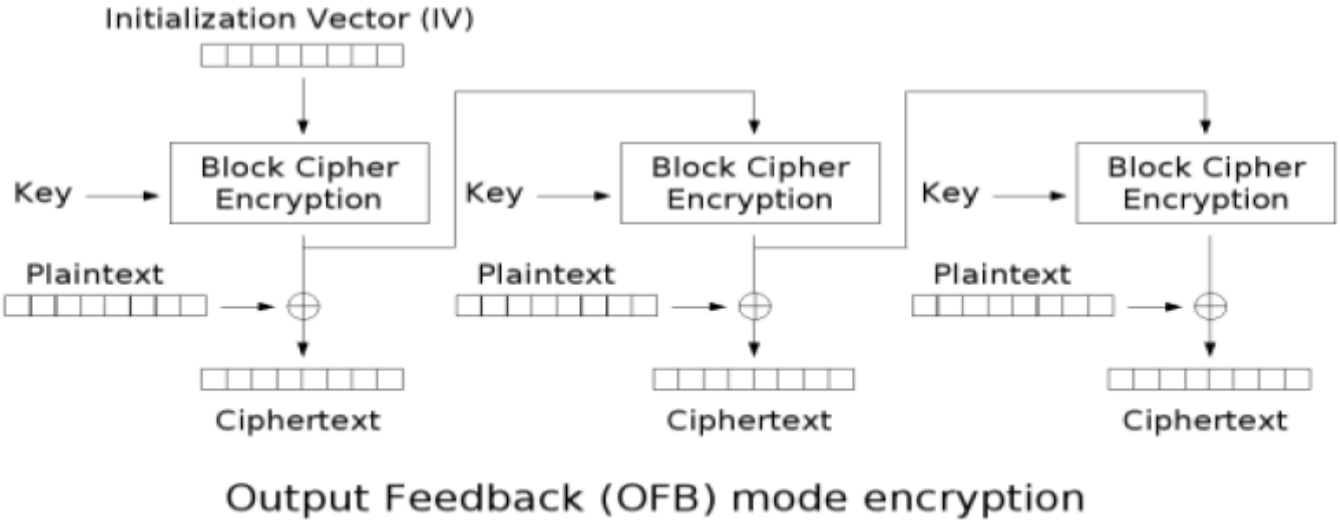


Αποκρυπτογράφηση CBC (ΕΑΠ ΠΛΗ35 - 3η ΟΣΣ Γιάννης Μαυρίδης)

CFB & OFB

OFB
Ένα λάθος του ενός bit στο κρυπτογραφημένο κείμενο θα προκαλέσει ένα λανθασμένο bit του αρχικού κειμένου, καθώς πρόκειται για αλγόριθμο ροής.





Κρυπτογράφηση CFB & OFB (ΕΑΠ ΠΛΗ35 - 3η ΟΣΣ Γιάννης Μαυρίδης)

Αλγόριθμος DES

Πληροφορίες Δέσμες αρχικού και κρυπτοκειμένου : 64 bits
Μήκος κλειδιού K: 56 bits (56 bits + 8 bits ισοτιμίας) Συνολικό πλήθος πιθανών κλειδιών: 2^{56}
Πρόβλημα ασφάλειας λόγω του μικρού μήκους κλειδιού.

Λειτουργία
Αρχική μετάθεση (Initial Permutation) των bit της δέσμης σύμφωνα με τον πίνακα 3.2(a). Το 58ο bit γίνεται πρώτο, το 50ο δεύτερο, το 42ο τρίτο κ.λ.π.

Ακολουθείται παρόμοια διαδικασία (PC-1) με τα bit του κλειδιού σύμφωνα με τον πίνακα 3.4(b) αφού έχουν αφαιρεθεί τα 8 bit (τελευταία στήλη, πίνακας 3.4(a)).

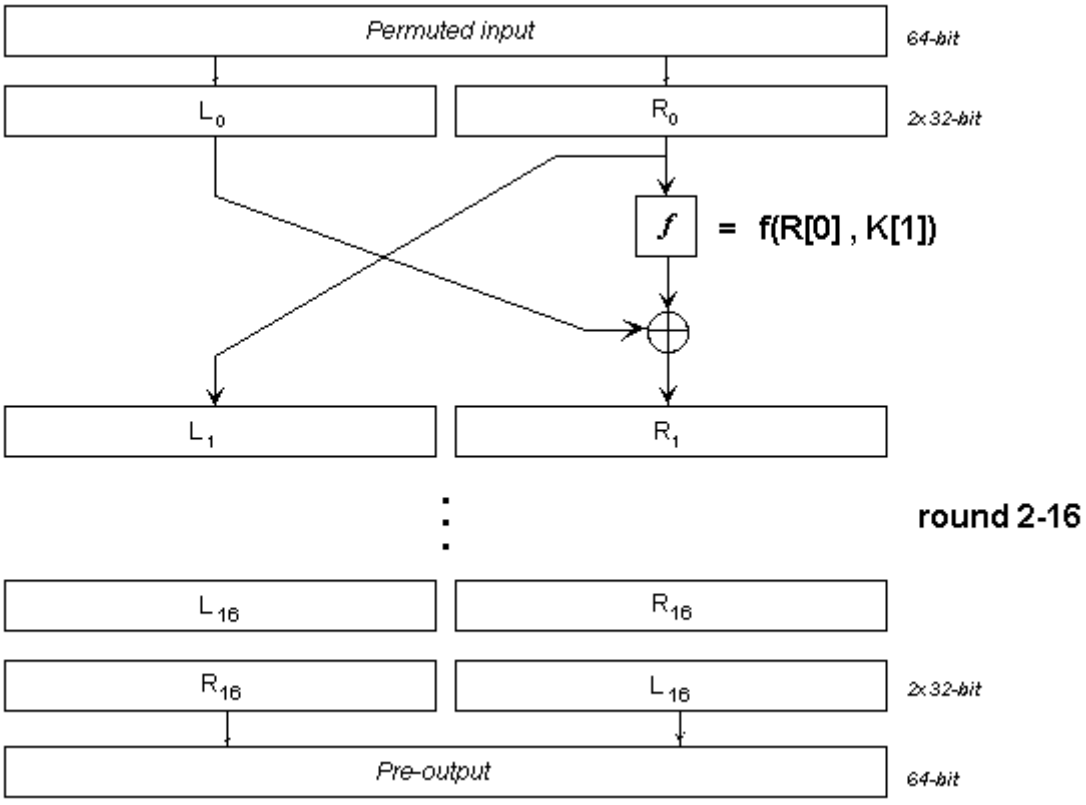
Χωρισμός του πίνακα στη μέση σε L και R (4 σειρές ο κάθε ένας) πίνακας 3.4(b). Παραγωγή 16 48-bit υποκλειδιών : Αριστερή Μετατόπιση για τα bit του L και R - Για να κάνουμε μια αριστερή μετατόπιση, μετακινούμε κάθε bit κατά μία θέση προς τα αριστερά, εκτός από το πρώτο bit, το οποίο μεταφέρεται στο τέλος του μπλοκ.

Στήλη 1 $\rightarrow$	**Στήλη 8**
1 $\rightarrow$	1
1 $\rightarrow$	0
0 $\rightarrow$	1
1 $\rightarrow$	1

*Ουσιαστικά αλλάζει μόνο η 1 με αλλαγή του πρώτου bit και μεταφορά στην 8. Οι υπόλοιπες μετατίθενται μια θέση αριστερά. (2,3,4,5,6,7,8,**1**)*

Ακολουθεί ένωση των L και R και εκ νέου μετάθεση (PC-2) σύμφωνα με τον πίνακα 3.4(c). Το αποτέλεσμα είναι το πρώτο υποκλειδί με 8 bits λιγότερα (48 bits).

Ακολουθεί η κύρια λειτουργία του Αλγορίθμου DES.
16 γύροι. Για κάθε γύρο ένα υποκλειδί πραγματοποιεί κρυπτογράφηση σε συγκεκριμένο block.
Μετά την αρχική μετάθεση η δέσμη εισόδου χωρίζεται σε δύο δέσμες των 32 bit L_0 και R_0. Για κάθε γύρο $i = 1, \ldots, 16$ έχουμε $L_i = R_{i-1}$ και $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$, όπου K_i είναι το κλειδί για το γύρο i.



Συνάρτηση f
Τα R_{i-1} (32 bits) πρέπει να επεκταθούν ώστε να γίνει η πράξη **XOR** με το αντίστοιχο K_i (48 bits), οποίο γίνεται κατά τον πίνακα 3.2(c).

Η επέκταση Ε γίνεται **XOR** με το υποκλειδί K_i του γύρου. Το αποτέλεσμα χωρίζεται σε 8 block των 6 bit $\mathrm{B}[1], \mathrm{B}[2], \mathrm{B}[3], \mathrm{B}[4], \mathrm{B}[5], \mathrm{B}[6], \mathrm{B}[7], \mathrm{B}[8]$.
Ο κάθε αριθμός υποδηλώνει ποιό **S-box (πίνακας 3.3)** θα χρησιμοποιηθεί στο αντίστοιχο block. Για κάθε block $\mathrm{B}[i]$ το πρώτο και τελευταίο bit υποδηλώνει την γραμμή στο αντίστοιχο S-box ενώ τα τέσσερα μεσαία υποδηλώνουν την στήλη (δυαδική αναπαράσταση). Παράδειγμα $\mathrm{B}[1]$ = 110110. Τότε το πρώτο bit είναι το 1 και το τελευταίο bit είναι το 0, οπότε η γραμμή είναι το 10 $\rightarrow$ 2 (**Προσοχή!! η αρίθμηση σε γραμμές / στήλες ξεκινά από το 0**). Τα μεσαία bit είναι 1011 $\rightarrow$ 11. Από το S-box 1, γραμμή 2 - στήλη 11, έχουμε το 7 $\rightarrow$ 0111.

Πραγματοποιείται αντικατάσταση στα $B[i]$ με τα αποτέλεσματα. Και έχουμε τον πίνακα R με γραμμές τα νέα $B[i]$.
Τέλος πραγματοποιείται αναμετάθεση στον R σύμφωνα με τον πίνακα 3.2(d). Το αποτέλεσμα είναι το $f(R[i-1], K[i])$ για το γύρο i.

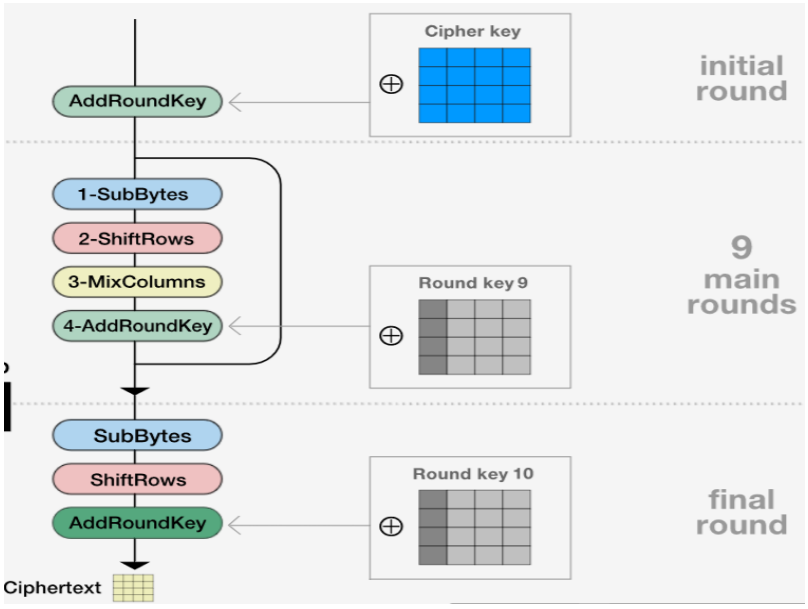
Τελικά βήματα
Αφού ολοκληρωθούν οι 16 γύροι έχουμε ενα αποτέλεσμα στο οποίο γίνεται μετάθεση (IP^{-1}) σύμφωνα με τον πίνακα 3.2(b). Το αποτέλεσμα αυτού είναι το κρυπτογραφημένο μήνυμα σε block.

Αλγόριθμος AES

Πληροφορίες Δέσμες αρχικού block : 128 bit
Μήκος κλειδιού : 128, 192, 256 bit
Πλήθος γύρων (ανάλογα με το μήκος κλειδιού) : 10, 12, 14

Λειτουργία
4x4 πίνακες για τις πληροφορίες, 16-byte, 4 bytes = 1 λέξη.

Το κλειδί προεκτείνεται σε $n+1$ γύρους και κάθε κλειδί χρησιμοποιείται για ένα γύρο.
Αρχικά το block εισόδου γίνεται XOR με το κλειδί. Έπειτα παιρνάμε σε επαναλαμβανόμενους $n-1$ γύρους.



Rijndael Animation

Επαναλαμβανόμεοι γύροι

SubBytes

Αντικατάσταση σύμφωνα με τον παρακάτω πίνακα Sbox.

	x0	x1	x2	x3	x4	x5	x6	x7	x8	x9	xa	xb	xc	xd	xe	xf
0x	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1x	ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
2x	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3x	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4x	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5x	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6x	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7x	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8x	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9x	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
ax	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
bx	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
cx	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
dx	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
ex	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
fx	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Rhee MY. Internet security: cryptographic principles, algorithms and protocols. Hoboken, NJ: J. Wiley, 2003

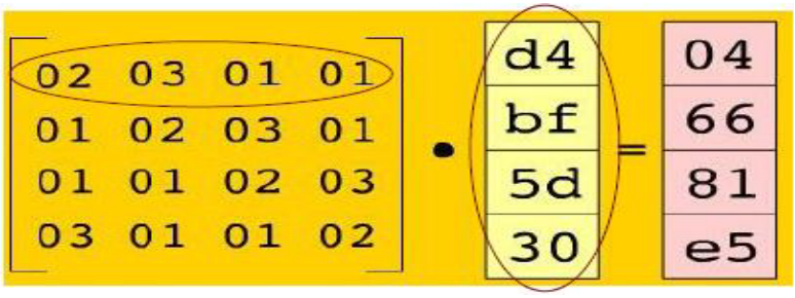
ShiftRows

Μετάθεση κάθε byte του block αριστερά.

Η 2η γραμμή κατα 1 θέση, η 3η γραμμή κατα 2 θέσεις, η 4η γραμμή κατα 3 θέσεις.

MixColumns

- Mix Columns
  - πρόσθεση με XOR
  - 03 = 02 XOR 01
  - πολλαπλασιασμός επί 2 (in Rijndael's Galois Field)
    - αν το αριστερότερο bit είναι 0:
      - 1-bit left shift (<< 1)
    - αν το αριστερότερο bit είναι 1:
      - 1-bit left shift (<< 1)
      - XOR με (00011011)

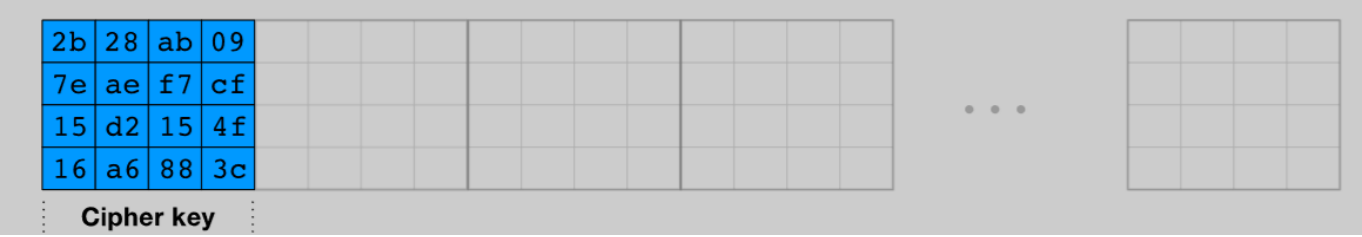


Κρυπτογράφηση CFB & OFB (ΕΑΠ ΠΛΗ35 - 3η ΟΣΣ Γιάννης Μαυρίδης)

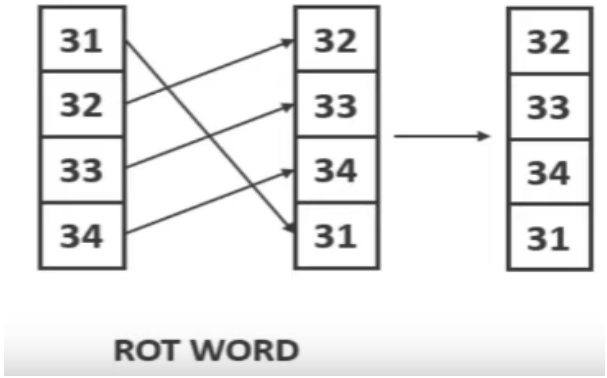
AddRoundKey

XOR με το κλειδί στήλη με στήλη.

Επέκταση κλειδιών



Οι στήλες που είναι πολ/σια του 4 υπολογίζονται με μετάθεση μίας θέσης πάνω όπως φαίνεται στην κάτω είκονα.



Έπειτα πραγματοποιείται η αντικατάσταση με τον πίνακα Sbox. Τέλος πραγματοποιείται XOR με την $i-4$ στήλη του επεκταμένου κλειδιού και XOR με την επόμενγ στήλη του πίνακα Rcon (η οποία και αφαιρείται από τον πίνακα).

RCON

01	02	04	08	10	20	40	80	1B	36
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00
00	00	00	00	00	00	00	00	00	00

Οι υπόλοιπες στήλες υπολογίζονται με XOR με την προηγούμενη στήλη και την $i-4$ στήλη του επεκταμένου κλειδιού.

Ασύμμετρη κρυπτογραφία - Κρυπτογραφία δημοσίου κλειδιού

Σε ένα δίκτυο με n κόμβους, για την ανά δύο ασφαλή επικοινωνία τους, χρειάζονται **ΣΥΝΟΛΙΚΑ** $2n$ κλειδιά.
(**Προσοχή!! Ένα δημόσιο και ένα ιδιωτικό για κάθε κόμβο, ανταλλάσονται μόνο τα δημόσια**).

Αλγόριθμος εδραίωσης κλειδιού Diffie-Hellman (DH)

Λειτουργία

Έστω πρώτος p και γεννήτορας (πρωτογενής ρίζα του p) $g \in Z_p$
Η Alice επιλέγει τον τυχαίο αριθμό $a \in Z_p^*$ και στέλνει στον Bob το (p, g, $g^a mod p$).
Ο Bob επιλέγει τον τυχαίο αριθμό b και απαντά στην Alice με ($g^b mod p$).
Τέλος και οι δύο μπορούν να υπολογίσουν μυστικό κλειδί που να χρησιμοποιήσουν για να κρυπτογραφήσουν μηνύματα $(g^a mod p)^b \equiv (g^b mod p)^a \equiv g^{ab} mod p$

Προβλήματα ασφάλειας

Καθώς δεν υπάρχει επιβεβαίωση για την ταυτότητα προέλευσης των μηνυμάτων ο αλγόριθμος είναι ευάλωτος σε επιθέσεις ενδιάμεσου. Η Mallory μπορεί να επεμβαίνει ανάμεσα στην Alice και στον Bob και να κάνει ανταλλαγή κλειδιού και με τους δύο κάνοντάς τους να υποθέτουν πως μιλούν μεταξύ τους. Αυτό θα μπορούσε να αντιμετωπιστεί εφαρμόζοντας κάποιο μηχανισμό αυθεντικοποίσης όπως πιστοποιητικά για τα $g^a mod p$ και $g^b mod p$ τα οποία εκδίδονται από τις αρχές πιστοποίησης.

Αλγόριθμος RSA

p, q ικανοποιητικά μεγάλοι τυχαία επιλεγμένοι πρώτοι.

Υπολογισμοί

$n = pq$
$\phi(n) = (p-1)(q-1)$
Επιλογή e με $gcd(\phi(n), e) = 1; 1 < e < \phi(n)$ (Επομένως ποτέ ζυγός αριθμός)
Επαλήθευση επιλεγμένου e ώστε $e, \phi(n)$ πρώτοι μεταξύ τους με τον αλγόριθμο του Ευκλείδη (βλέπε κάτω πίνακα, παράληψη τελευταίας στήλης)

Υπολογισμός d

$d \equiv e^{-1} (mod \phi(n))$

Αλγόριθμος Ευκλείδη (Παράδειγμα για $e = 7$ και $\phi(n) = 120$)

a	**b**	a_i **/** b_i	$amodb$	$amodb = a_i - b_i$
$\phi(n) = 120$	$e = 7$	17	1	$1 = 1 \cdot 120 - 17 \cdot 7$
7	1	7	0	

$gcd(120, 7) = 1 = 1 \cdot 120 - 17 \cdot 7$
Έτσι $d \equiv x (mod \phi(n)) = x (mod (p-1) \cdot (q-1)) = -17 (mod 120) = 103$
Υπολογισμός αρνητικού modulo: $-17 (mod 120) = 120 - 17 (mod 120) = 120 - 17 = 103$

Υπολογισμός e με γνωστό d

$d \cdot e \equiv 1 (mod \phi(n))$

Κλειδιά

Δημόσιο Κλειδί: $\{e, n\}$
Ιδιωτικό Κλειδί: $\{d, n\}$

Κρυπτογράφηση

Εξίσωση: $c \equiv m^e (mod n)$
Παράδειγμα για μήνυμα 6425, block = 2, $e = 7$ *και* $n = 143$
$64^7 mod 143 = 103$
$25^7 mod 143 = 64$
Άρα το κρυπτογραφημένο μήνυμα είναι $c = 103\ 64$

Αποκρυπτογράφηση

Εξίσωση: $m \equiv c^d (mod n)$
Παράδειγμα για μήνυμα 103 64, $d = 103$ *και* $n = 143$
$103^{103} mod 143 = 64$
$64^{103} mod 143 = 25$
Άρα το αποκρυπτογραφημένο μήνυμα είναι $m = 64\ 25$

Αλγόριθμος El-Gamal

Αρχικά επιλέγεται πρώτος p και γεννήτορας α του Z_p (primitive root of p)
Έπειτα επιλέγεται από τον χρήστη Α τυχαίος αριθμος k έτσι ώστε $1 <= k <= p - 1$ (στο βιβλίο αναφέρεται ως S_A)
Υπολογίζεται το δημόσιο κλειδί y (στο βιβλίο αναφέρεται ως P_A) από την σχέση $y = a^k mod p$, το οποίο και δημοσιοποιείται.
Ο χρήστης Β για να στείλει το μήνυμα Μ επιλέγει τυχαίο αριθμό r έτσι ώστε $1 <= r <= p - 1$. Έπειτα υπολογίζεται το κρυπτογραφικό κλειδί K από την σχέση $\mathrm{K} = y^r mod p$. Τέλος υπολογίζεται το ζεύγος $(C1, C2)$, με τις σχέσεις $C1 = a^r mod p$ και $C2 = K \cdot M mod p$, το οποίο αποτελεί την κρυπτογραφημένη μορφή του μηνύματος Μ.
Ο χρήστης Α όταν παραλάβει το κρυπτογράφημα $(C1, C2)$, υπολογίζει το κλειδί K από την σχέση $K = C1^k mod p$ και αποκρυπτογραφεί το μήνυμα με την σχέση $M = (C2/\mathrm{K}) mod p$.