Ασφάλεια Συστημάτων

Τζέριες Μπεσαράτ, PhD

20 Μαΐου 2022, Άρτα

Στο προηγούμενο μάθημα αναπτύξαμε

- Κρυπτογραφία
  - Κρυπτογραφικό Σύστημα
  - Κρυπτανάλυση
  - Κλειδί
  - Αλγόριθμοι Κρυπτογράφησης
- Στεγανογραφία
- Χρήσιμες Έννοιες
- Μελέτη κλασσικών κρυπτογραφικών αλγορίθμων
  - Αλγόριθμος του Καίσαρα
  - Αλγόριθμος Vigenere

Σύγχρονοι Κρυπτογραφικοί Αλγόριθμοι

Η εφαρμογή των δύο κλασσικών κρυπτογραφικών αλγορίθμων που εξετάστηκαν στο προηγούμενο κεφάλαιο είναι εφικτή μόνο σε κείμενα, δηλαδή σε συμβολοσειρές. Επίσης η διαδικασία της κρυπτανάλυσης είναι σχετικά απλή και οδηγεί σε αποτελέσματα σε σύντομο χρονικό διάστημα.

Στην περίπτωση που το μήνυμα το οποίο αποστέλλεται από τη μία οντότητα στην άλλη, έχει μια σύνθετη μορφή (π.χ. εκτελέσιμο πρόγραμμα) και οι ανάγκες εμπιστευτικότητας είναι αυξημένες, επιβάλλεται η ψηφιακή επεξεργασία με την εφαρμογή σύγχρονων κρυπτογραφικών αλγορίθμων που έχουν σχεδιαστεί με αντικείμενο τις ανάγκες των σύγχρονων επικοινωνιακών συστημάτων

Θα δούμε

- Συμμετρικά Κρυπτοσυστήματα
  - DES
  - AES
  - Τρόποι Λειτουργίας
- Ασύμμετρα Κρυπτοσυστήματα
  - RSA
- Μελέτη Σύγχρονων Αλγόριθμων

Το βασικό σενάριο σε μια κρυπτογραφημένη επικοινωνία είναι:

- Έστω δύο επικοινωνούντα μέρη, που τα ονομάζουμε Αλίκη και Βασίλη.
- Η Αλίκη κρυπτογραφεί το αρχικό κείμενο Μ χρησιμοποιώντας ένα κλειδί Κ και παράγει το κρυπτοκείμενο C.
- Το κρυπτοκείμενο C μεταδίδεται στον Βασίλη, ο οποίος το παραλαμβάνει και το αποκρυπτογραφεί για να ανακτήσει το αρχικό κείμενο Μ, εφόσον γνωρίζει το κλειδί αποκρυπτογράφησης.
- Ένας κακόβουλος χρήστης, έστω η Ελένη, μπορεί να καταφέρει να υποκλέψει το κρυπτοκείμενο, ωστόσο ο αλγόριθμος κρυπτογράφησης θα πρέπει να εγγυάται ότι δεν πρόκειται να καταφέρει να το μετατρέψει σε μια μορφή κατανοητή ώστε να μπορέσει να το διαβάσει, διαφυλάσσοντας έτσι τη μυστικότητα του μεταδιδόμενου μηνύματος

Συμμετρικά Κρυπτοσυστήματα

Τρεις από τους πιο γνωστούς συμμετρικούς αλγορίθμους, που χρησιμοποιούνται σήμερα ευρέως είναι:

- Ο αλγόριθμος DES (Data Encryption Standard),
- η μετεξέλιξή του 3DES (triple-DES) και
- ο νεώτερος αλγόριθμος AES (Advanced Encryption Standard).

DES

Ο κρυπτογραφικός αλγόριθμος Data Encryption Standard (DES) είναι ένας συμμετρικός αλγόριθμος δέσμης, ο οποίος υιοθετήθηκε ως το επίσημο πρότυπο (Federal Information Processing Standard) FIPS 46 των ΗΠΑ το
1977.

Το 1973, στο πλαίσιο ενός προγράμματος που είχε ξεκινήσει ένα χρόνο νωρίτερα, ο οργανισμός NIST (τότε γνωστός ως NBS) δημοσίευσε μια πρόσκληση για υποβολή προτάσεων για ένα νέο αλγόριθμο συμμετρικού κλειδιού, ο οποίος θα αποτελούσε το νέο πρότυπο κρυπτογράφησης σε εθνικό επίπεδο και θα έπρεπε να πληροί κάποια κριτήρια.

Τα κριτήρια

- Να παρέχει υψηλό επίπεδο ασφάλειας.
- Να είναι πλήρως τεκμηριωμένος και εύκολα κατανοητός
- Η ασφάλειά του να βασίζεται στο κλειδί και όχι στη μυστικότητα του ίδιου του αλγορίθμου.
- Να είναι διαθέσιμος σε όλους τους χρήστες.
- Να είναι προσαρμόσιμος για χρήση σε ποικίλες εφαρμογές.
- Να είναι υλοποιήσιμος με χαμηλό κόστος.
- Να είναι αποδοτικός.
- Να μπορεί να επικυρωθεί.

Ο αλγόριθμος DES δέχτηκε επικρίσεις για δύο κυρίως λόγους:

- Διέθετε μικρό μήκος κλειδιού (56 bits), αρκετά μειωμένο σε σχέση με το κλειδί μήκους 128 bit του Lucifer. Το γεγονός αυτό καθιστούσε τον αλγόριθμο ευάλωτο σε επιθέσεις εξαντλητικής αναζήτησης (brute-force attacks).
- Υπήρχε μυστικότητα και αδιαφάνεια σχετικά με κάποιο τμήμα του σχεδιασμού της εσωτερικής δομής του. Οι επικριτές υποστήριζαν πως το τμήμα της αρχιτεκτονικής του αλγόριθμου που αφορούσε τα S-box (θα παρουσιαστούν στη συνέχεια), τα οποία προέκυψαν από μεταβολή αυτών του Lucifer, επέτρεπε την ύπαρξη «κερκόπορτας» (backdoor), ώστε να παρέχεται η δυνατότητα άμεσης αποκρυπτογράφησης, χωρίς την ανάγκη της γνώσης του κάθε επιμέρους μυστικού κλειδιού. Αργότερα, οι συμμετέχοντες ερευνητές δήλωσαν πως οι αλλαγές στην εσωτερική δομή αφορούσαν όντως μόνο τα S-box, αλλά έγιναν στο πλαίσιο μιας προσπάθειας απομάκρυνσης ορισμένων ευπαθειών που αναγνωρίσθηκαν κατά τη διαδικασία επιβεβαίωσης (validation) του αλγορίθμου.

Περιγραφή DES

Ο DES είναι ένας αλγόριθμος που υλοποιεί μια δομή Feistel με 16 κύκλους εκτέλεσης.

Σε κάθε κύκλο χρησιμοποιείται ένα υποκλειδί μήκους 48 bit, που παράγεται από το μυστικό κλειδί.

Το τελευταίο εκφράζεται συνήθως με τη χρήση 64bit, από τα οποία όμως κάθε όγδοο bit αγνοείται καθώς χρησιμοποιείται μόνο για έλεγχο ισοτιμίας.

Το αρχικό κείμενο διαχωρίζεται σε δέσμες (block) των 64 bit και παράγονται δέσμες κρυπτοκειμένου του ίδιου μήκους (64 bit).

Αντιστρόφως, κατά την αποκρυπτογράφηση, οι δέσμες κρυπτοκειμένου μήκους 64 bit αποτελούν, μαζί με το ίδιο μυστικό κλειδί, την είσοδο στη διαδικασία αποκρυπτογράφησης και παράγονται δέσμες αρχικού κειμένου με μήκος πάλι 64 bit.

Μεθοδολογία δημιουργίας υποκλειδιών

Για να παραχθούν τα 16 κλειδιά μήκους 48bit, ακολουθείται η εξής διαδικασία:

1. Στο αρχικό κλειδί μήκους 64bit, εφαρμόζεται μια αρχική μετάθεση (permutation), όπου κάθε όγδοο bit αγνοείται και τα υπόλοιπα 56 επανατοποθετούνται, σύμφωνα με τον πίνακα PC1 (Permuted Choice One)

C	57	49	41	33	25	17	9
	1	58	50	42	34	26	18
	10	2	59	51	43	35	27
	19	11	3	60	52	44	36
D	63	55	47	39	31	23	15
	7	62	54	46	38	30	22
	14	6	61	53	45	37	29
	21	13	5	28	20	12	4

Μεθοδολογία δημιουργίας υποκλειδιών

2. Στη συνέχεια, το κλειδί των 56bit χωρίζεται σε δυο τμήματα: το αριστερό C0 και το δεξί D0, μήκους 28bit
3. Σε κάθε έναν από τους 16 κύκλους εκτέλεσης του DES:
    - Τα τμήματα Ci-1 και Di-1 υπόκεινται σε κυκλική αριστερή ολίσθηση, κατά
        - 1 bit στους κύκλους 1, 2, 9 και 16,
        - 2 bit σε όλους τους υπόλοιπους.
    - Στα τμήματα Ci και Di συνενώνονται και εφαρμόζεται μια τελική επιλογή και μετάθεση, σύμφωνα με τον πίνακα PC2 (Permuted Choice Two) για να προκύψει το υποκλειδί Ki του κύκλου, μήκους 48 bits

C	57	49	41	33	25	17	9
	1	58	50	42	34	26	18
	10	2	59	51	43	35	27
	19	11	3	60	52	44	36
D	63	55	47	39	31	23	15
	7	62	54	46	38	30	22
	14	6	61	53	45	37	29
	21	13	5	28	20	12	4

Πίνακας PC1.

14	17	11	24	1	5	3	28
15	6	21	10	23	19	12	4
26	8	16	7	27	20	13	2
41	52	31	37	47	55	30	40
51	45	33	48	44	49	39	56
34	53	46	42	50	36	29	32

Πίνακας PC2.

Επεξεργασία δέσμης αρχικού κειμένου

Ο αλγόριθμος DES επεξεργάζεται ένα αρχικό κείμενο, αφού πρώτα το χωρίσει σε δέσμες μήκους 64 bit. Σε κάθε δέσμη εφαρμόζεται μια αρχική μετάθεση (Initial Permutation), σύμφωνα με τον πίνακα αρχικής μετάθεσης IP.

Μετά την αρχική μετάθεση, η κάθε δέσμη χωρίζεται σε δύο υποδέσμες, την αριστερή L_0 που αποτελείται από τα πρώτα 32 bit και τη δεξιά R_0 που αποτελείται από τα υπόλοιπα 32.

Πίνακας IP

L_0	58	50	42	34	26	18	10	2
	60	52	44	36	28	20	12	4
	62	54	46	38	30	22	14	6
	64	56	48	40	32	24	16	8
R_0	57	49	41	33	25	17	9	1
	59	51	43	35	27	19	11	3
	61	53	45	37	29	21	13	5
	63	55	47	39	31	23	15	7

Επεξεργασία δέσμης αρχικού κειμένου

Οι υποδέσμες L_0 και R_0 γίνονται είσοδοι σε μια δομή Feister με 16 κύκλους επεξεργασίας, όπου στον i-οστό κύκλο έχουμε:

- Η δεξιά υποδέσμη γίνεται η επόμενη αριστερή υποδέσμη ($L_i = R_{i-1}$).
- Εφαρμόζεται μετάθεση και επέκταση της δεξιάς υποδέσμης R_{i-1}, ώστε να αποκτήσει μήκος 48bit, σύμφωνα με τον πίνακα Επέκτασης Μετάθεσης (Expansion Permutation)
- Υπολογίζεται η πράξη XOR με εισόδους τα R_{i-1} και K_i

Πίνακας επέκτασης Ε

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

Επεξεργασία δέσμης αρχικού κειμένου

- Το αποτέλεσμα της πράξης XOR, μήκους 48bit, χωρίζεται σε 8 εξάδες και κάθε μια χρησιμοποιείται ως είσοδος ενός από τα 8 S-box (αντίστοιχος πίνακας), το οποίο παράγει έξοδο μήκους 4bit, ως εξής:
  - Από την εξάδα bit, επιλέγεται το πρώτο και το έκτο bit για να διαμορφώσουν μια δυάδα bit, η οποία καθορίζει τη γραμμή του S-box
  - Από την εξάδα bit, επιλέγονται τα τέσσερα ενδιάμεσα bit για να διαμορφώσουν μια δυάδα bit, η οποία καθορίζει τη στήλη του S-box
  - Το περιεχόμενο του κελιού του S-box που καθορίζεται από την παραπάνω γραμμή και στήλη, θα αποτελέσει την έξοδο του S-box.

Έτσι, αν η εξάδα 100110 αποτελέσει την είσοδο του πρώτου S-box (S1), τότε θα επιλεγεί το περιεχόμενο του κελιού, που αντιστοιχεί στη δεύτερη γραμμή (10) και στην τρίτη στήλη (0011), είναι 8.
Άρα, στην έξοδο το αποτέλεσμα θα είναι τα bit: 1000. Για την επιλογή γραμμής και στήλης θυμηθείτε ότι μετράμε ξεκινώντας από το μηδέν (0).

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
S_2	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Επεξεργασία δέσμης αρχικού κειμένου

- Στη συνέχεια, οι οκτώ τετράδες από bit συνενώνονται (συνολικά 8x4 = 32bit) και εφαρμόζεται μια τελική μετάθεση, σύμφωνα με τον πίνακα μετάθεσης P (αντίστοιχος πίνακας), για να προκύψει η νέα δεξιά υποδέσμη R_{i-1}.
- Η επόμενη δεξιά υποδέσμη προκύπτει από τον υπολογισμό της πράξης XOR με εισόδους τα R_{i-1} και L_{i-1} ($R_i = R_{i-1} \oplus L_{i-1}$).
- Στα 64 bit που τελικά προκύπτουν από τη συνένωση των υποδεσμών L_{16} και R_{16}, εφαρμόζεται μια μετάθεση, σύμφωνα με τον ανάστροφο πίνακα της αρχικής μετάθεσης (Inverse Permutation – IP^{-1}), ώστε να προκύψει η κρυπτογραφημένη δέσμη.

Πίνακες Μετάθεσης P και Ανάστροφος πίνακας της αρχικής μετάθεσης

16	7	20	21	29	12	28	17
1	15	23	26	5	18	31	10
2	8	24	14	32	27	3	9
19	13	30	6	22	11	4	25

Πίνακας μετάθεσης P.

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

Πίνακας Inverse Permutation IP^{-1}.

3DES

Όπως αναφέρθηκε παραπάνω, το μικρό σε μέγεθος μήκος κλειδιού του DES διευκολύνει τις επιθέσεις εξαντλητικής αναζήτησης (brute-force attack).

Η αρχική προσέγγιση προς τη βελτίωση του αλγορίθμου ήταν η χρήση ενός δεύτερου, ώστε το αποτέλεσμα της πρώτης κρυπτογράφησης με DES να κρυπτογραφείται εκ νέου με DES αλλά με το δεύτερο κλειδί, ώστε από το αρχικό μήνυμα M να προκύψει το κρυπτογράφημα $C=E_{DES}(K_2, E_{DES}(K_1,M))$. Με αυτό τον τρόπο, υλοποιείται ο Double DES και το μήκους του κλειδιού πλέον θεωρείται ότι αυξήθηκε στα 112bit.

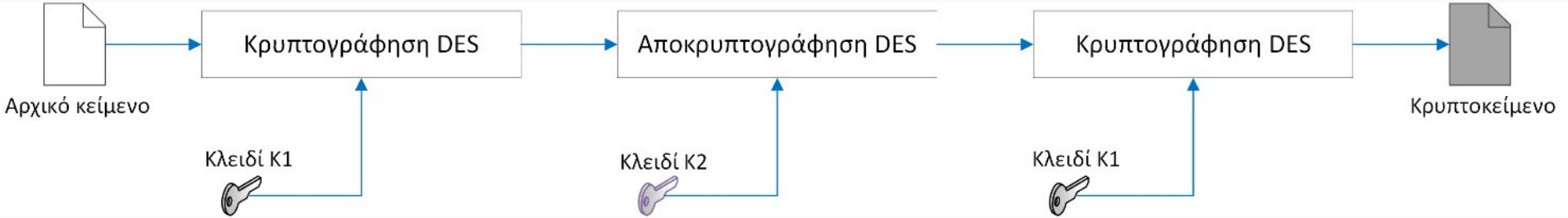
Τα προβλήματα που ενδέχεται να παρουσιάζει η προσέγγιση αυτή είναι:

- Η περίπτωση να υπάρχει κλειδί K', τέτοιο ώστε $C=E_{DES}(K_2, E_{DES}(K_1,M))= E_{DES}(K', M)$. Στην περίπτωση αυτή θα αρκούσε η εύρεση ενός κλειδιού K'. Η περίπτωση αυτή έχει αποκλειστεί από τους Campbell και Wiener το 1992.

- Είναι δυνατό να υπάρχει $X=E_{DES}(K_1,M)=D_{DES}(K_2,C)$. Για ένα γνωστό ζεύγος M, C, κρυπτογραφούμε το M για κάθε πιθανή τιμή του K_1. Στη συνέχεια, αποκρυπτογραφούμε το C με κάθε πιθανή τιμή του K_2. Αν από τη διαδικασία προκύψουν δύο ίδια αποτελέσματα υποθέτουμε πως έχουμε εντοπίσει τα κλειδιά K_1 και K_2. Η επίθεση αυτή, γνωστή Meet-in-themiddle είναι ο βασικότερος λόγος εγκατάλειψης του Double DES και υιοθέτησης του 3DES (Triple-DES)

Για την αντιμετώπιση της επίθεσης αυτής, προτάθηκε η χρήση τριών επιπέδων κρυπτογράφησης

Συγκεκριμένα, το κρυπτογράφημα προκύπτει από μια διαδικασία κρυπτογράφησης με το κλειδί K_1, αποκρυπτογράφησης με το κλειδί K_2 και εκ νέου κρυπτογράφησης με το K_1, όπως φαίνεται στην Εικόνα.
Με τον τρόπο αυτό, ο χώρος αναζήτησης αυξάνει στα 2^{112} κλειδιά.



AES

Το 1997, ο οργανισμός NIST ξεκίνησε την αναζήτηση του αντικαταστάτη του αλγορίθμου DES. Στις προδιαγραφές που καθορίσθηκαν, περιλαμβάνονταν τα εξής σημεία:

- Ο αλγόριθμος θα έπρεπε να είναι αδιαβάθμητος και ελεύθερα διαθέσιμος.
- Ο αλγόριθμος θα έπρεπε να είναι συμμετρικός αλγόριθμος δέσμης.
- Ο αλγόριθμος θα έπρεπε να υποστηρίζει κλειδιά μεταβλητού μήκους 128, 192 και 256 bits.

Από το σύνολο των αλγορίθμων που προτάθηκαν, προκρίθηκαν στη δεύτερη φάση αξιολόγησης οι ακόλουθοι πέντε:

- MARS, της εταιρίας IBM (ΗΠΑ).
- RC6, του οργανισμού RSA Laboratories (ΗΠΑ).
- Rijndael, των ερευνητών Joan Daemen και Vincent Rijmen (Βέλγιο).
- Serpent, των ερευνητών Ross Anderson (ΗΒ), Eli Bihar (Ισραήλ), και Lars Knudsen (Νορβηγία).
- Twofish, των ερευνητών Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, και Niels Ferguson (ΗΠΑ).

Από την αξιολόγηση, μεγαλύτερη βαθμολογία έλαβε τελικά ο αλγόριθμος Rijndael, με το όνομά του να αποδίδεται σε λογοπαίγνιο με τα επώνυμά των ερευνητών που τον πρότειναν.

Παράμετροι λειτουργίας του αλγόριθμου Rijndael

Μήκος Κλειδιού (Word/Byte/Bit)	4/16/128	6/24/192	8/32/256
Μήκος Δέσμης (Word/Byte/Bit)	4/16/128	4/16/128	4/16/128
Πλήθος κύκλων επεξεργασίας	10	12	14
Μήκος Υποκλειδιού (Word/Byte/Bit)	4/16/128	4/16/128	4/16/128

Ο κρυπτογραφικός αλγόριθμος Rijndael προτυποποιήθηκε με την ονομασία Advanced Encryption Standard (AES) (FIPS 197) για μήκος κλειδιού και δέσμης στα 128 bit και παρουσιάστηκε από τον οργανισμό National Institute of Standards and Technology (NIST) το 2001.

Ιδιότητες AES

- αντοχή σε όλες τις μέχρι τότε γνωστές επιθέσεις,
- ταχύτητα εκτέλεσης και οικονομία κώδικα κατά την υλοποίηση σε όλες τις διαθέσιμες πλατφόρμες,
- απλότητα στη σχεδίαση

Τοποθέτηση byte σε πίνακα State.

01	23	45	67	89	AB	CD	EF	FE	DC	BA	98	76	54	32	10

01	89	FE	76
23	AB	DC	54
45	CD	BA	32
67	EF	98	10

Η κρυπτογράφηση με χρήση του AES ακολουθεί τα βήματα:

- Επέκταση του μυστικού κλειδιού σε υποκλειδιά.
- Μια αρχική πρόσθεση (XOR) υποκλειδιού (AddRoundKey).
- Έναν αριθμό κύκλων που περιλαμβάνει την αντικατάσταση byte (Sub Bytes), την ολίσθηση γραμμών (Shift Rows), την ανάμειξη byte (Mix Bytes) και την πρόσθεση υποκλειδιού (AddRoundKey).
- Ένα τελικό κύκλο που περιλαμβάνει την αντικατάσταση byte (Sub Bytes), την ολίσθηση γραμμών (Shift Rows) και την πρόσθεση υποκλειδιού (AddRoundKey).

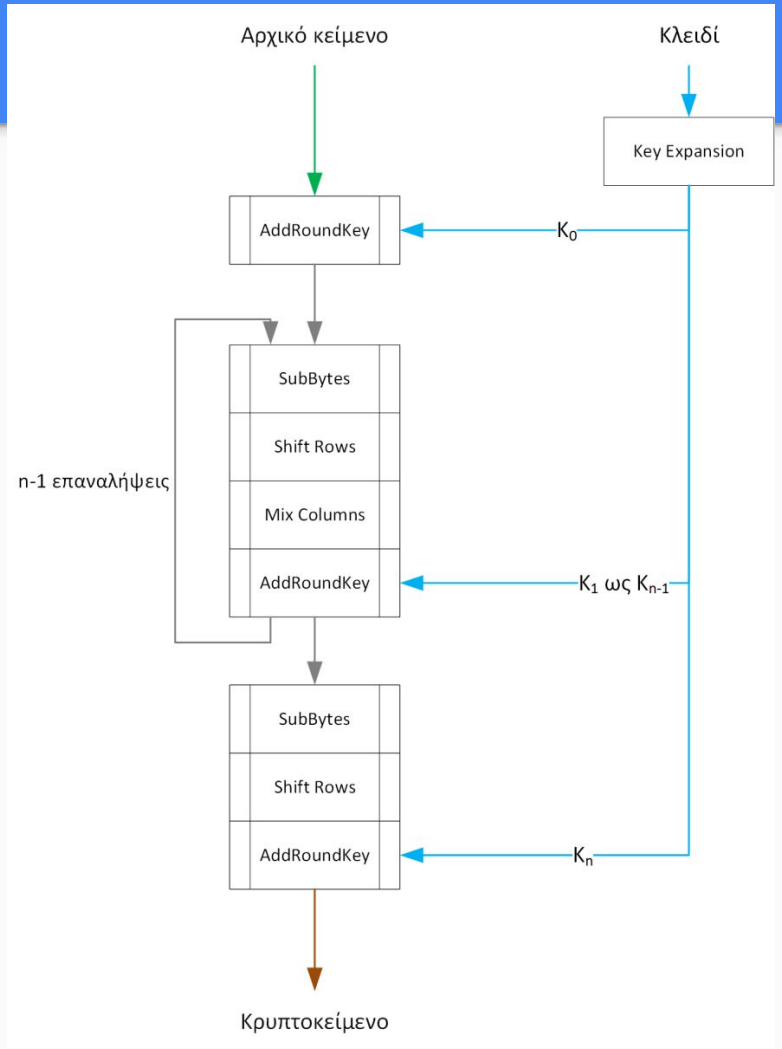
Ο αριθμός των κύκλων επεξεργασίας καθορίζεται από το μήκος της δέσμης και το μήκος του κλειδιού.

Αριθμός απαιτούμενων κύκλων

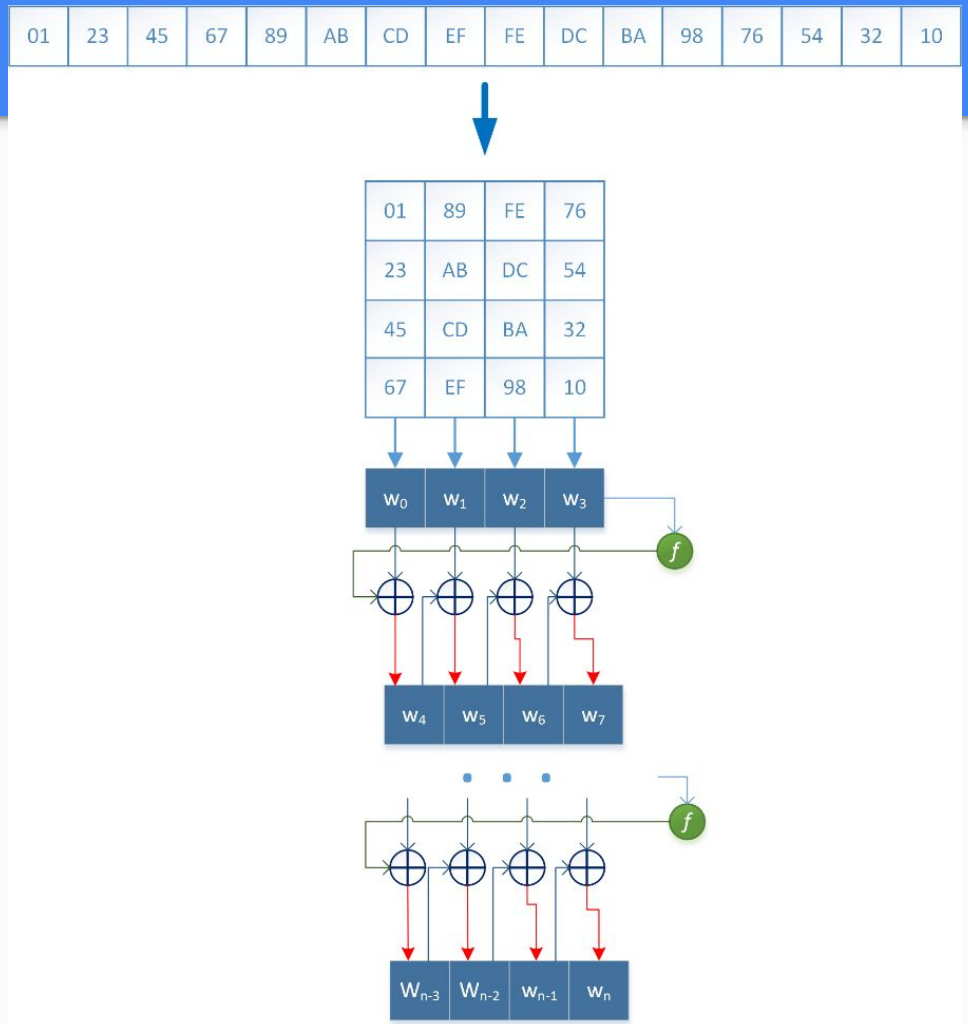
	Κλειδί 128 bit	**Κλειδί 192 bit**	**Κλειδί 256 bit**
Δέσμη 128 bit	10	12	14
Δέσμη 192 bit	12	12	14
Δέσμη 256 bit	14	14	14

Ομοίως με παραπάνω, καθώς ο AES προτυποποιεί τον αλγόριθμο Rijndael για μήκος δέσμης των 128 bit, μπορούμε να έχουμε 10, 12 ή 14 κύκλους για μήκος κλειδιού 128, 192 και 256 bits αντίστοιχα.

Συνοπτική παρουσίαση του AES



Διαδικασία επέκτασης κλειδιού



Τρόποι λειτουργίας

- Electronic Codebook (ECB)
- Cipher Block Chaining (CBC)
- Cipher FeedBack Mode (CFB)
- Output FeedBack Mode (OFB)

Ασύμμετρα Κρυπτοσυστήματα

Οι ασύμμετροι κρυπτογραφικοί αλγόριθμοι βασίζονται κυρίως στη χρήση μαθηματικών πράξεων και για αυτό ενδείκνυνται για την κρυπτογράφηση / αποκρυπτογράφηση αριθμητικών δεδομένων, μικρού μεγέθους.

Για την ασφάλεια των ΤΠΕ γίνεται συμπληρωματική αξιοποίηση των συμμετρικών και των ασύμμετρων κρυπτογραφικών αλγορίθμων προκειμένου να παρέχονται ολοκληρωμένες και αποδοτικές υπηρεσίες ασφάλειας.

3 κατηγορίες στις οποίες μπορούμε να εντάξουμε τα κρυπτοσυστήματα δημοσίου κλειδιού:

- Κρυπτογράφηση/αποκρυπτογράφηση: Ο αποστολέας κρυπτογραφεί το μήνυμα με το δημόσιο κλειδί του παραλήπτη, ο οποίος το αποκρυπτογραφεί με το ιδιωτικό του κλειδί. Με αυτό τον τρόπο προστατεύεται η εμπιστευτικότητα του μηνύματος.
- Ψηφιακή υπογραφή: Ο αποστολέας υπογράφει το μήνυμα κρυπτογραφώντας το με το ιδιωτικό κλειδί του. Ο παραλήπτης επιβεβαιώνει την ψηφιακή υπογραφή αποκρυπτογραφώντας το κρυπτοκείμενο με το δημόσιο κλειδί του αποστολέα. Η υπογραφή μπορεί να γίνει στο σύνολο του μηνύματος ή μόνο σε ένα μικρό σετ δεδομένων το οποίο παράγεται ως αποτέλεσμα της εφαρμογής μιας συνάρτησης κατακερματισμού (hashing function) πάνω στο σύνολο του μηνύματος. Με αυτό τον τρόπο προστατεύεται η αυθεντικότητα του αποστολέα και η ακεραιότητα του μηνύματος.
- Ανταλλαγή κλειδιών: Τα δύο επικοινωνούντα μέρη συνεργάζονται ώστε να ανταλλάξουν με ασφάλεια (εξασφαλίζοντας την εμπιστευτικότητα) ένα συμμετρικό κλειδί συνόδου.

Αλγόριθμοι δημοσίου κλειδιού.

Από τους γνωστούς αλγόριθμους κάποιοι είναι κατάλληλοι και για τις τρεις κατηγορίες κρυπτογραφικών ενεργειών, ενώ άλλοι για λιγότερες. Στον παρακάτω πίνακα εμφανίζονται με συνοπτικό τρόπο οι δυνατότητες των πιο γνωστών αλγόριθμων δημόσιου κλειδιού:

Αλγόριθμος	**Κρυπτογράφηση**	**Ψηφιακή Υπογραφή**	**Ανταλλαγή Κλειδιών**
RSA	ΝΑΙ	ΝΑΙ	ΝΑΙ
Diffie - Hellman	ΟΧΙ	ΟΧΙ	ΝΑΙ
DSS	ΟΧΙ	ΝΑΙ	ΟΧΙ
Elliptic Curves	ΝΑΙ	ΝΑΙ	ΝΑΙ

RSA

Ένας από τους πρώτους αλγορίθμους δημοσίου κλειδιού που αναπτύχθηκαν ήταν ο RSA. Το ακρωνύμιο προκύπτει από τα ονόματα των Ron Rivest, Adi Shamir, και Len Adleman που πρότειναν τον συγκεκριμένο αλγόριθμο το 1977.

Σύμφωνα με τον αλγόριθμο RSA, η κρυπτογράφηση γίνεται σε δέσμες (blocks) αρχικού κειμένου, το περιεχόμενο των οποίων είναι μια αριθμητική τιμή που πρέπει να είναι μικρότερη από έναν αριθμό n.