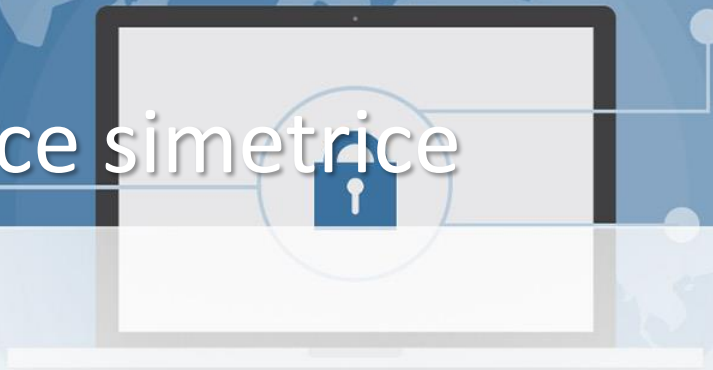
Criptografie și Securitate Cibernetică

CSC – RCC 2

Conținut

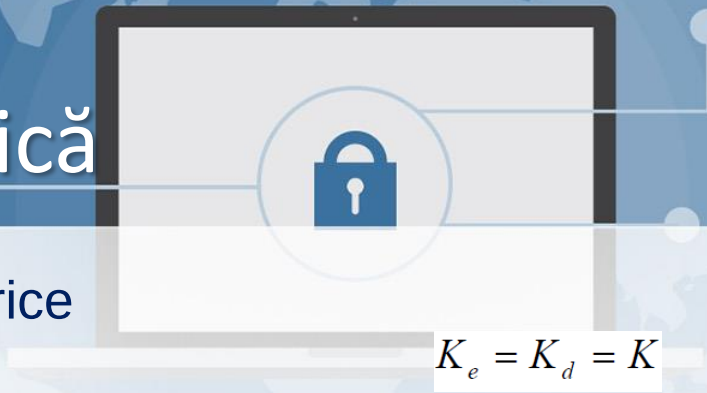
- Sisteme criptografice simetrice
  - Tehnici clasice de criptate
  - Cifruri pe blocuri
  - Sistemul de criptare DES
  - Alternative DES
  - Sistemul de criptare AES
- Sisteme criptografice asimetrice
  - Tehnici
  - Cifruri cu cheie publică
  - Sistemul de criptare RSA
  - Criptografia cu chei publice
  - Criptarea cu chei publice
  - Semnătura digitală

Sisteme criptografice simetrice



- Tehnici clasice de criptate
- Cifruri pe blocuri
- Sistemul de criptare DES
- Alternative DES
- Sistemul de criptare AES

Criptografia simetrică



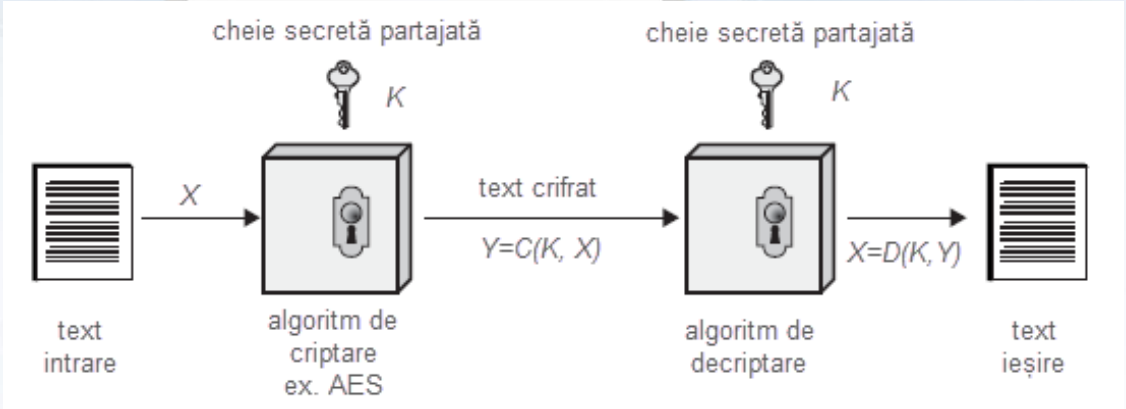
$$K_e = K_d = K$$

- Criptosisteme cu chei simetrice
- (cu cheie secretă)
- (criptosisteme convenţionale)
  - cheile folosite la criptare şi decriptare sunt identice
- Clasificare după tipul algoritmului
  - *cu cifruri bloc (block ciphers)*

    operațiile de criptare (substituție și transpoziție) acționează asupra unei diviziuni a textului inițial
  - cu cifruri secvențiale *(stream ciphers)*
- mesajul de la intrare este considerat ca o succesiune (şir) de simboluri, criptarea făcându-se simbol cu simbol

Modelul criptografic simetric

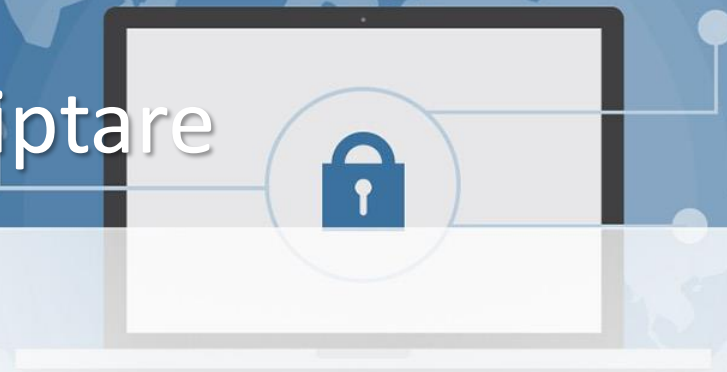
- Componente
  - Text original
  - Algoritm de criptare
  - Cheie secretă
  - Text criptat
  - Algoritm de decriptare



Cerințe

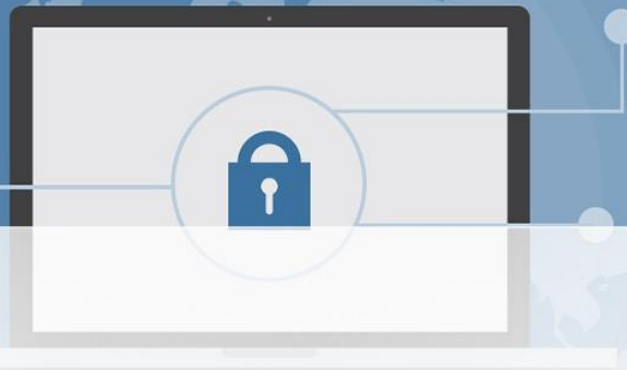
- Algoritm de criptare puternic
- Aceeași cheie la expeditor și destinatar
- Transmitere sigură

Tehnici de Criptare



- Metode de criptare
  - Substituție
    - ✓literele din textul original sunt înlocuite cu alte litere, de numere sau simboluri
  - Transpoziție
    - ✓literele din textul original sunt reordonate literele, fără a le schimba (ascunde)
  - Combinate
    - ✓combinații între substituție și transpoziție

Cifruri cu substituţie



- Cifrul de substituţie
- (*substituion cipher*)
  - fiecare caracter sau grup de caractere ale textului în clar (M) este substituit cu un alt caracter sau grup de caractere ale textului cifrat (C)
  - descifrarea făcându-se prin aplicarea substituţiei inverse asupra textului cifrat
- Atacuri
  - Analiza criptologică
  - Prin forța brută (*brute-force*)

Tipuri de cifruri cu substituţie

- Tipuri de cifruri de substituţie:
  - substituţie monoalfabetică (*monoalphabetic ciphers*)

    fiecare caracter al textului în clar (M) este înlocuit cu un caracter corespondent al textului cifrat (C) – ex. Cezar, Plybius
  - substituţie omofonică (*homophonic substitution ciphers*)

    un caracter al alfabetului mesajului în clar (alfabet primar) poate să aibă mai multe reprezentări (frecvența de apariție)
  - substituţie poligramică (*polygram substitution ciphers*)

    substituirea unor blocuri de caractere (poligrame) din textul clar, cu alte blocuri de caractere (SLL -> ABB) – ex. Playfair
  - substituţie polialfabetică

    formate din mai multe cifruri de substituţie simple - Vigenere, Autoclave, Vernam, Trithemius

Criptare prin substituție - exemple

- Cifrul Cezar
  - Înlocuiește fiecare literă din alfabet cu litera aflată cu 3 poziții mai departe

Text

```
plain:   a b c d e f g h i j k l m n o p q r s t u v w x y z
cipher:  D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
```

```
plain:   meet me after the toga party
cipher: PHHW PH DIWHU WKH WRJD SDUWB
```

Numeric

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

Generalizare

$$C = \mathrm{E}(3, p) = (p + 3) \bmod 26$$

$$C = \mathrm{E}(k, p) = (p + k) \bmod 26$$

$$p = \mathrm{D}(k, C) = (C - k) \bmod 26$$

Analiza criptografică

- Caracteristici ce facilitează
- decriptarea de tip „brute-force”
  - Cunoașterea algoritmului de criptare/decriptare
  - Sunt doar 25 chei care pot fi încercate
  - Limba textului original poate fi ușor de recunoscut
- Soluții
  - Extinderea alfabetului (ASCII)
  - Comprimarea textului (ZIP)
-

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozqsx
5	kccr kc ydrcp rfc rmey nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpan pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kvmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymxk max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rwkvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkbdi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzkx znk zumg vgxze
24	rjjy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevxc

Exemple de Cifruri cu substituție

- Criptare monoalfabetică extinsă (Cezar îmbunătățit)
  - În cifru poate fi orice permutare din cele 26 de caracterele alfabetice, atunci există 26! sau mai multe de chei posibile.
- Cifru substituţie poligramică – Cicru Play
  - Dispunerea alfabetului de 25 de litere (I=J) într-un pătrat de 5x5
    Prima linie e un cuvânt cheie
    Cifrarea se face pe grup de 2 litere

V	U	L	P	E
A	B	C	D	F
G	H	I	K	M
N	O	Q	R	S
T	W	X	Y	Z

- - dacă m1, m2 sunt dispuse în vârfurile opuse ale unui dreptunghi, atunci c1, c2 sunt caracterele din celelalte vârfuri ale dreptunghiului, c1 fiind în aceeaşi linie cu m1. De ex. GS devine MN
- - dacă m1 şi m2 se găsesc într-o linie, atunci c1 şi c2 se obţin printr-o deplasare ciclică spre dreapta a literelor m1 şi m2. De ex. AD devine BF sau CF devine DA
- - dacă m1 şi m2 se află în aceeaşi coloană atunci c1 şi c2se obţin prin deplasarea ciclică a lui
- m1, m2 de sus în jos. De ex. UO devine BW, iar EZ devine FE

Exemple de Cifruri cu substituție

- Criptare cu substituţie polialfabetică
  - formate din mai multe cifruri de substituţie simple
  - crește numărul cheilor la $(26!)^n$
- Ex. Cifrul lui Vigenère
  - cheia k este o secvenţă de litere
  - criptare
  - decriptare
  - exemplu

$$K = k_0, k_1, k_2, \ldots, k_{m-1}$$

$$C_i = (p_i + k_{i \bmod m}) \bmod 26$$

$$p_i = (C_i - k_{i \bmod m}) \bmod 26$$

```
key:          deceptivedeceptivedeceptive
plaintext:    wearediscoveredsaveyourself
ciphertext:   ZICVTWQNGRZGVTWAVZHCQYGLMGJ
```

key	3	4	2	4	15	19	8	21	4	3	4	2	4	15
plaintext	22	4	0	17	4	3	8	18	2	14	21	4	17	4
ciphertext	25	8	2	21	19	22	16	13	6	17	25	6	21	19

Cifruri de transpoziție

- *Transposition ciphers*
  - cifrurile cu transpoziţie reordonează literele, fără a le schimba
- Transpoziția pe coloane
  - textul sursă va fi scris literă cu literă şi apoi citit pe coloane, în ordinea dată de o anumită cheie
  - cheie poate fi un cuvânt cu litere distincte, de o lungime egală cu numărul de coloane folosite în cifru
  - ordinea alfabetică a literelor din cuvântul cheie va da ordinea în care se vor citi coloanele

N	E	E	D
H	E	L	P
F	A	S	T

textul rezultat este: ”NHFEEAELSDPT”

Exemple de Cifruri cu transpoziție

- Tehnica „*rail fence*”

  Text inițial “meet me after the toga party”

  Text criptat MEMATRHTGPRYETEFETEOAAT

```
m e m a t r h t g p r y
e t e f e t e o a a t
```

N	E	E	D
H	E	L	P
F	A	S	T

- Transpoziția pe coloane
- textul rezultat este: ”NHFEEAELSDPT”
- Schimbarea ordinei coloanelor

```
Key:          4 3 1 2 5 6 7
Plaintext:    a t t a c k p
              o s t p o n e
              d u n t i l t
              w o a m x y z
Ciphertext:   TTNAAPTMTSUOAODWCOIXKNLYPETZ
```

- Transpoziția multiplă

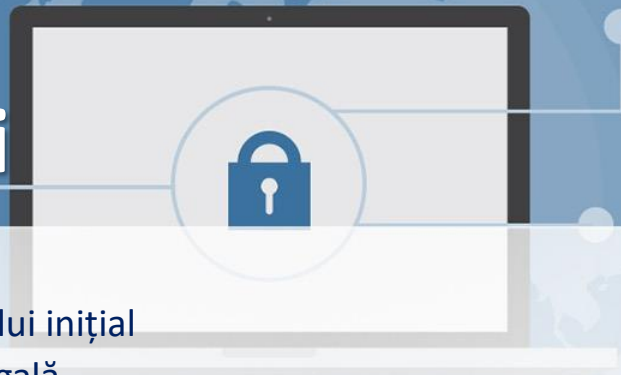
```
Key:          4 3 1 2 5 6 7
Input:        t t n a a p t
              m t s u o a o
              d w c o i x k
              n l y p e t z
Output:       NSCYAUOPTTWLTMDNAOIEPAXTTOKZ
```

MAŞINI ROTOR

- O maşină rotor (*rotor machine*)
  - are o tastatură şi o serie de rotoare ce permit implementarea unui cifru
  - fiecare rotor face o permutare arbitrară a alfabetului,
  - rotoarele au 26 de poziţii şi realizează o simplă substituţie
  - rotoarele se mişcă cu viteze de rotaţie diferite,
  - perioada unei maşini cu n rotoare este 26^n

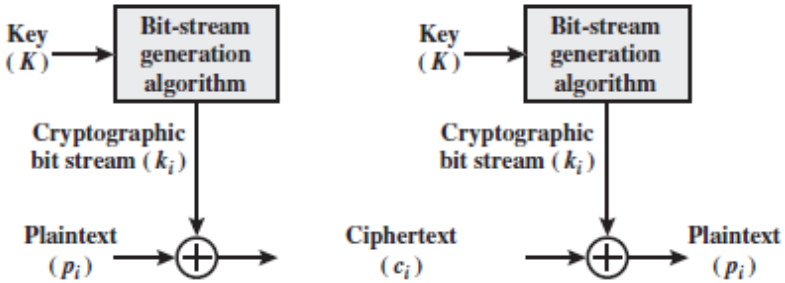
- Cel mai celebru cifru bazat pe o maşină rotor este Enigma,
- utilizată de germani în cel de-al doilea război mondial.

Cifruri bloc - Principii

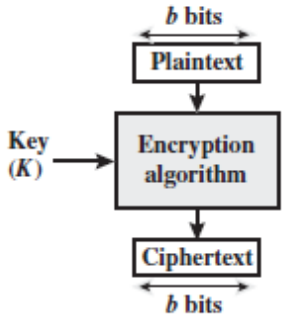


- Cifru bloc (*block ciphers*)
  - Tratează o parte/secțiune/diviziune a textului inițial
  - Produce prin criptare un bloc de lungime egală
- Caracteristici
  - Număr de runde identice de prelucrare
  - In fiecare rundă, este efectuată o schimbare pe o jumătate a datelor, urmată de o permutare între cele două jumătăți.
  - Cheia originală este extinsă, astfel că o altă cheie este folosită pentru fiecare rundă.
- EX. - Data Encryption Standard (DES)
  - a fost cel mai utilizat algoritm de criptare până de curând
  - folosește un bloc de 64 de biți și o cheie de 56 de biți
- Metode de criptanaliza
  - criptanaliza diferențială
    criptanaliza liniară

CRIPTARE
BLOC VS SECVENTIAL



(a) Stream cipher using algorithmic bit-stream generator

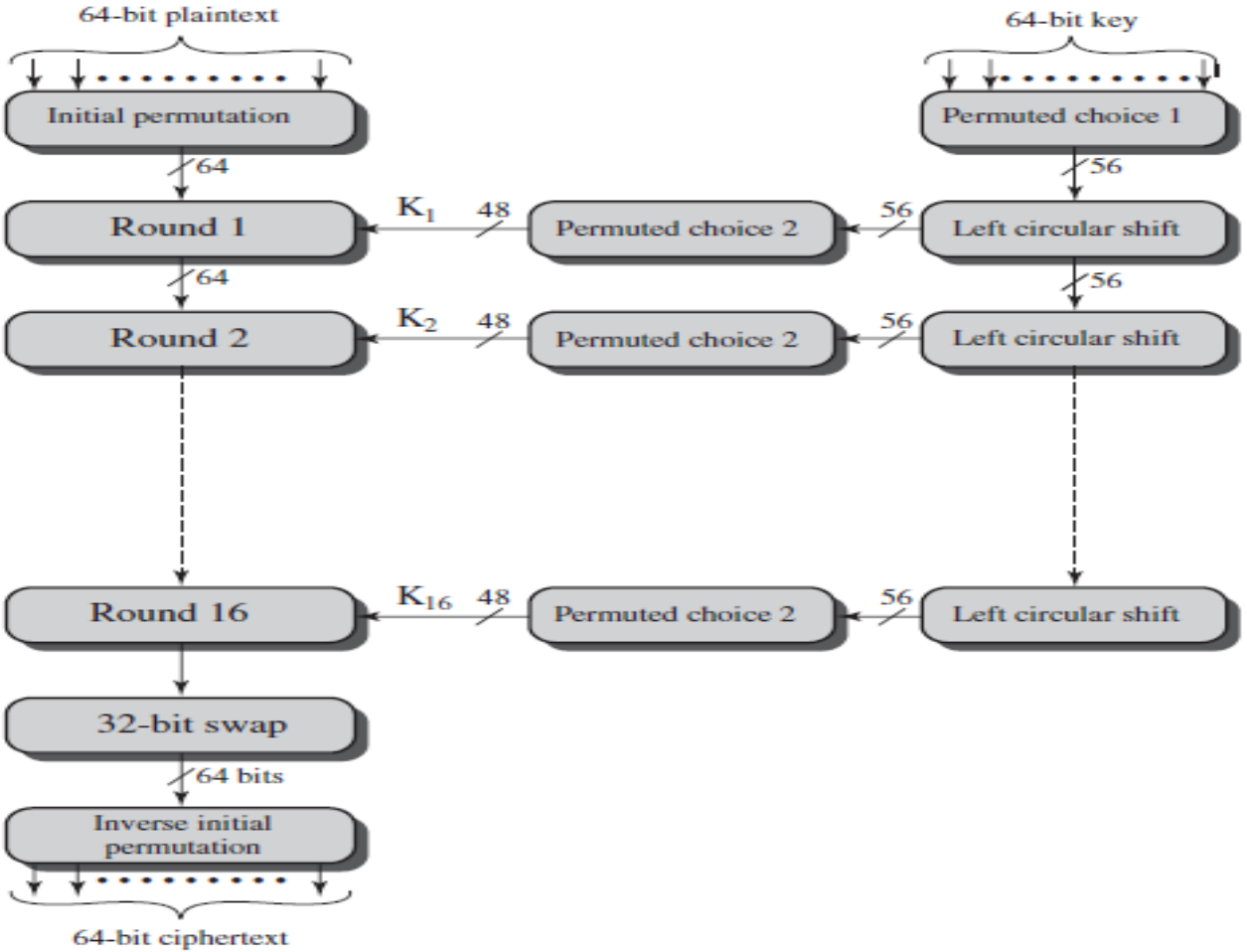


(b) Block cipher

Data Encryption Standard - DES

- Standardul de criptare a datelor (*Data Encryption Standard*)
  - Standard public
  - Implementabil în dispozitivele electronice
- Caracteristici
  - lungimea unui bloc este de 64 de biţi;
  - cheia este pe 64 de biţi dintre care 8 sunt biţi de paritate;
  - flexibilitatea implementării şi utilizării în diferite aplicaţii;
  - fiecare bloc cifrat este independent de celelalte;
  - nu este necesară sincronizarea între operaţiile de criptare/decriptare ale unui bloc;
- Creşterea securităţii
  - T-DES (triplu DES)
  - iterarea de trei ori a algoritmului DES

Diagramă DES



Permutări DES

(a) Initial Permutation (IP)

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
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

(b) Inverse Initial Permutation (IP^{-1})

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

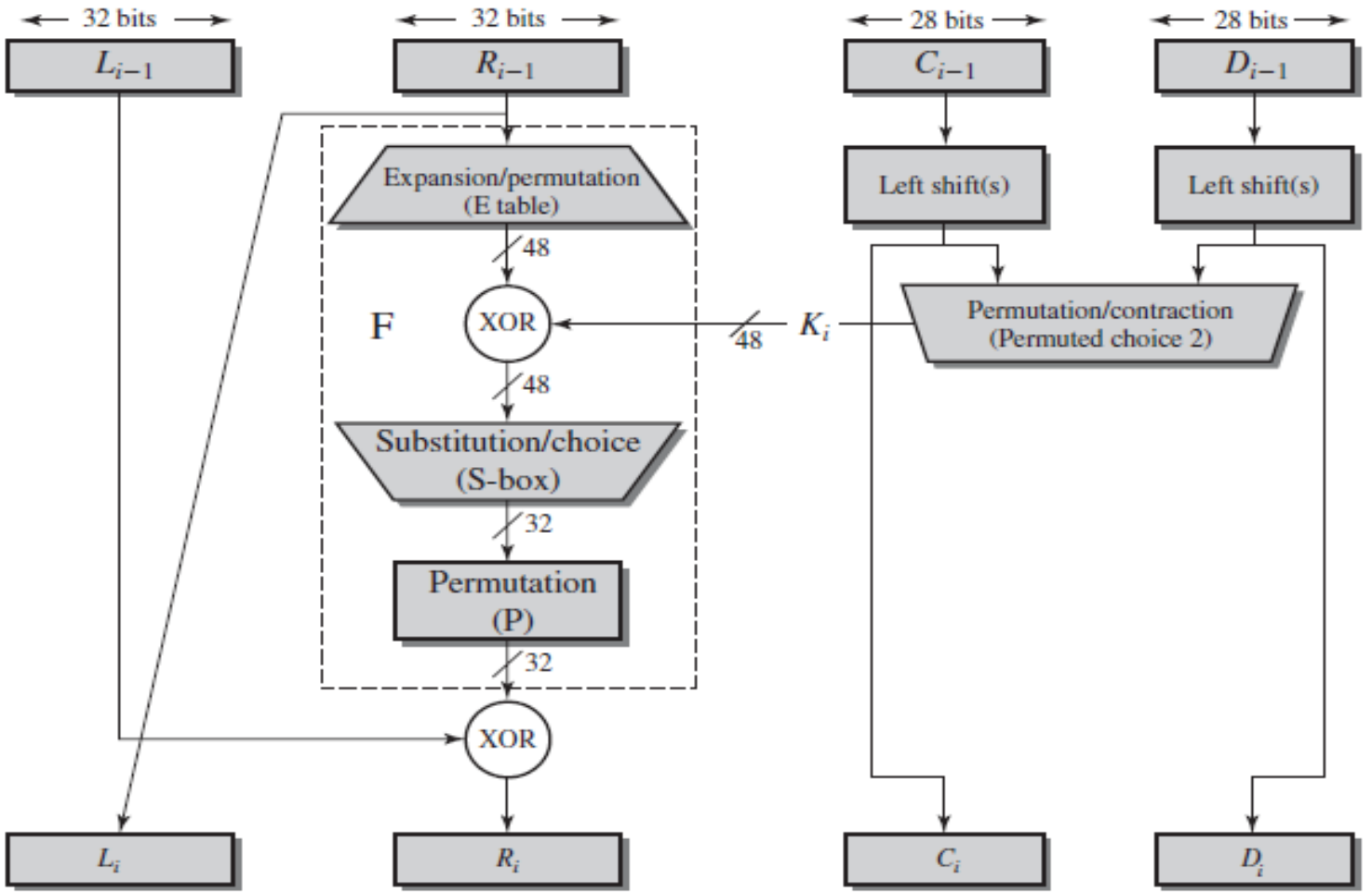
(c) Expansion Permutation (E)

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

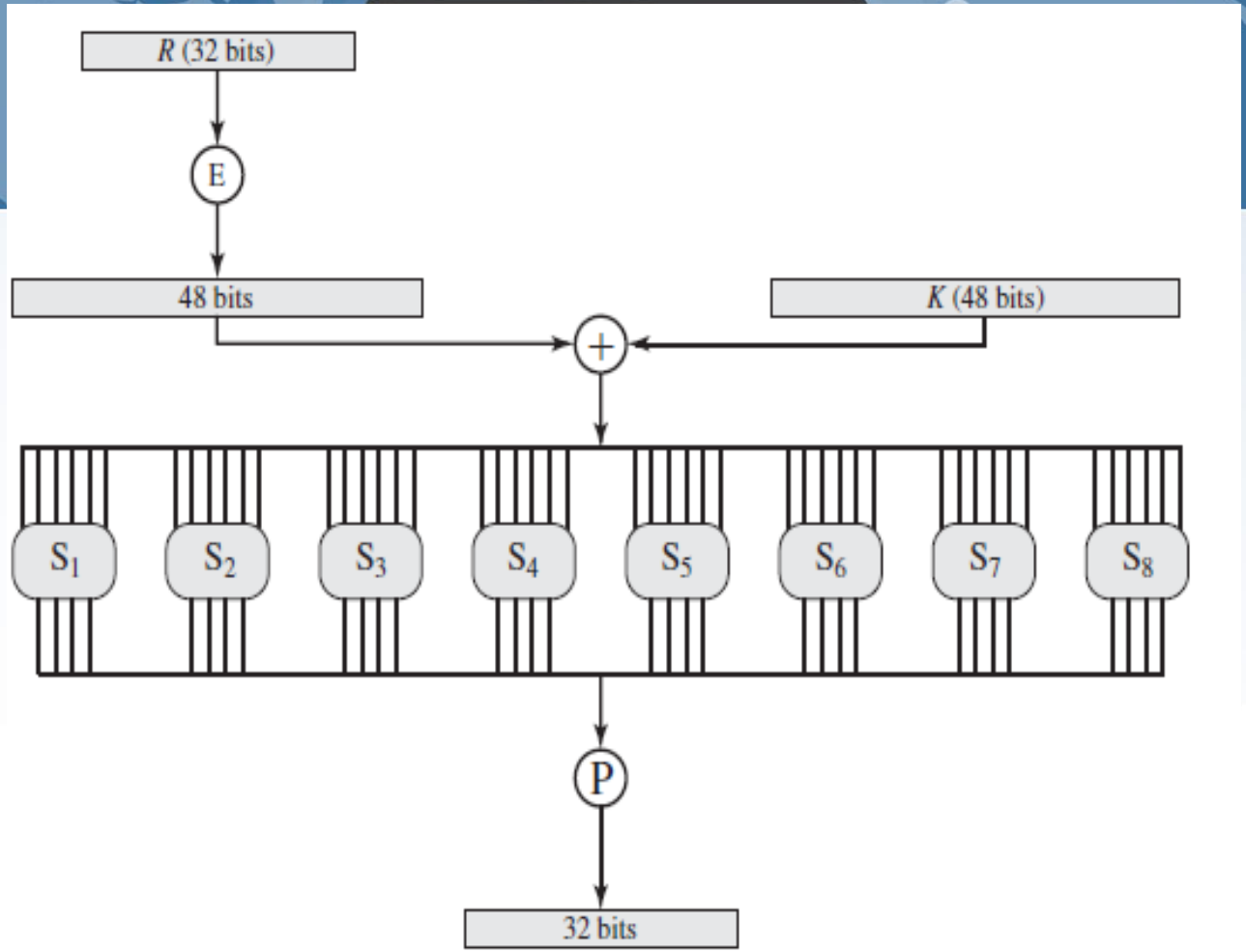
(d) Permutation Function (P)

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

Iterații DES



Funcția DES



Cutiile DES

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

Calcul cheie DES

(a) Input Key

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

(b) Permuted Choice One (PC-1)

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
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

(c) Permuted Choice Two (PC-2)

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

(d) Schedule of Left Shifts

Round Number	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Bits Rotated	1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

EXEMPLU DES

Plaintext:	02468aceeca86420
Key:	0f1571c947d9e859
Ciphertext:	da02ce3a89ecac3b

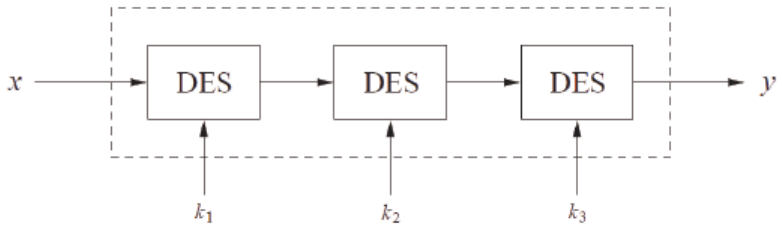
Round	K_i	L_i	R_i
IP		5a005a00	3cf03c0f
1	1e030f03080d2930	3cf03c0f	bad22845
2	0a31293432242318	bad22845	99e9b723
3	23072318201d0c1d	99e9b723	0bae3b9e
4	05261d3824311a20	0bae3b9e	42415649
5	3325340136002c25	42415649	18b3fa41
6	123a2d0d04262a1c	18b3fa41	9616fe23
7	021f120b1c130611	9616fe23	67117cf2
8	1c10372a2832002b	67117cf2	c11bfc09
9	04292a380c341f03	c11bfc09	887fbc6c
10	2703212607280403	887fbc6c	600f7e8b
11	2826390c31261504	600f7e8b	f596506e
12	12071c241a0a0f08	f596506e	738538b8
13	300935393c0d100b	738538b8	c6a62c4e
14	311e09231321182a	c6a62c4e	56b0bd75
15	283d3e0227072528	56b0bd75	75e8fd8f
16	2921080b13143025	75e8fd8f	25896490
IP^{-1}		da02ce3a	89ecac3b

Altenative DES

- Cheie de 56 biți - 2^56 = 7.2 x 10^16 valori
- Atacul brute-force (spart în cateva ore, în 2000)

- 3DES

$$y = DES_{k_3}(DES_{k_2}(DES_{k_1}(x)))$$

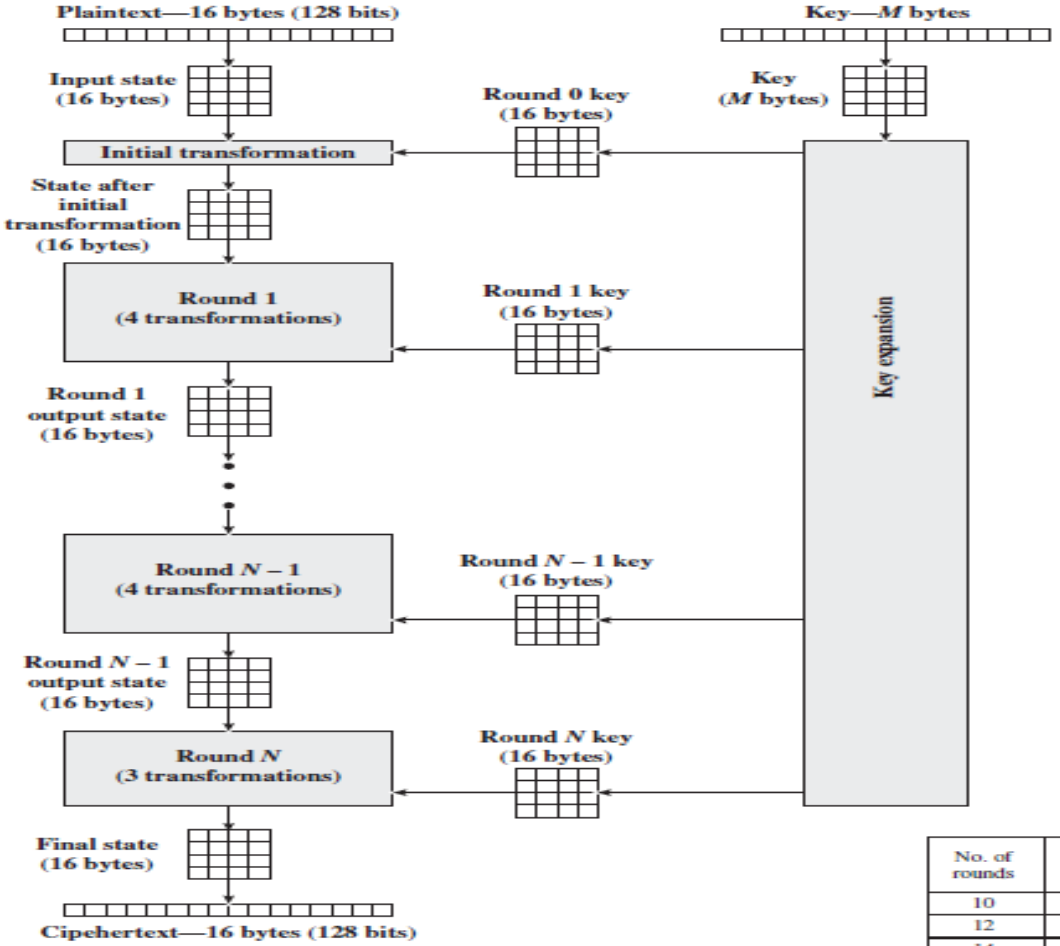


$$y = DES_{k_3}(DES_{k_2}^{-1}(DES_{k_1}(x)))$$

AES - Advanced Encryption Standard

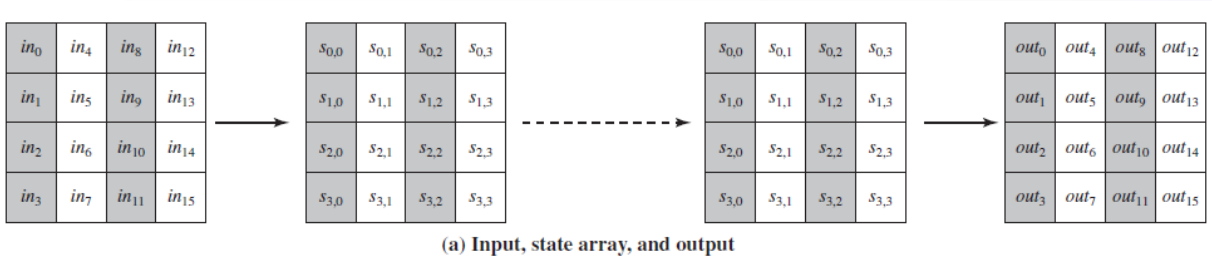
- Rijndael (Joan Daemen ¸si Vincent Rijman)
- cripteaza blocuri de text clar de lungime fixă
- folosind chei de 128, 192 sau 256 biti
- Nu se bazeaza pe structura Feistel
- Fiecare runda de criptare consta din 4 funcții separate
  - Substituție - ByteSub(Stare)
  - Permutare - ShiftRow(Stare)
  - Operații aritmetice - MixColumn(Stare)
  - XOR cu o cheie - AddRoundKey(Stare, Cheie)

Criptare AES



No. of rounds	Key Length (bytes)
10	16
12	24
14	32

STRUCTURĂ DATE AES

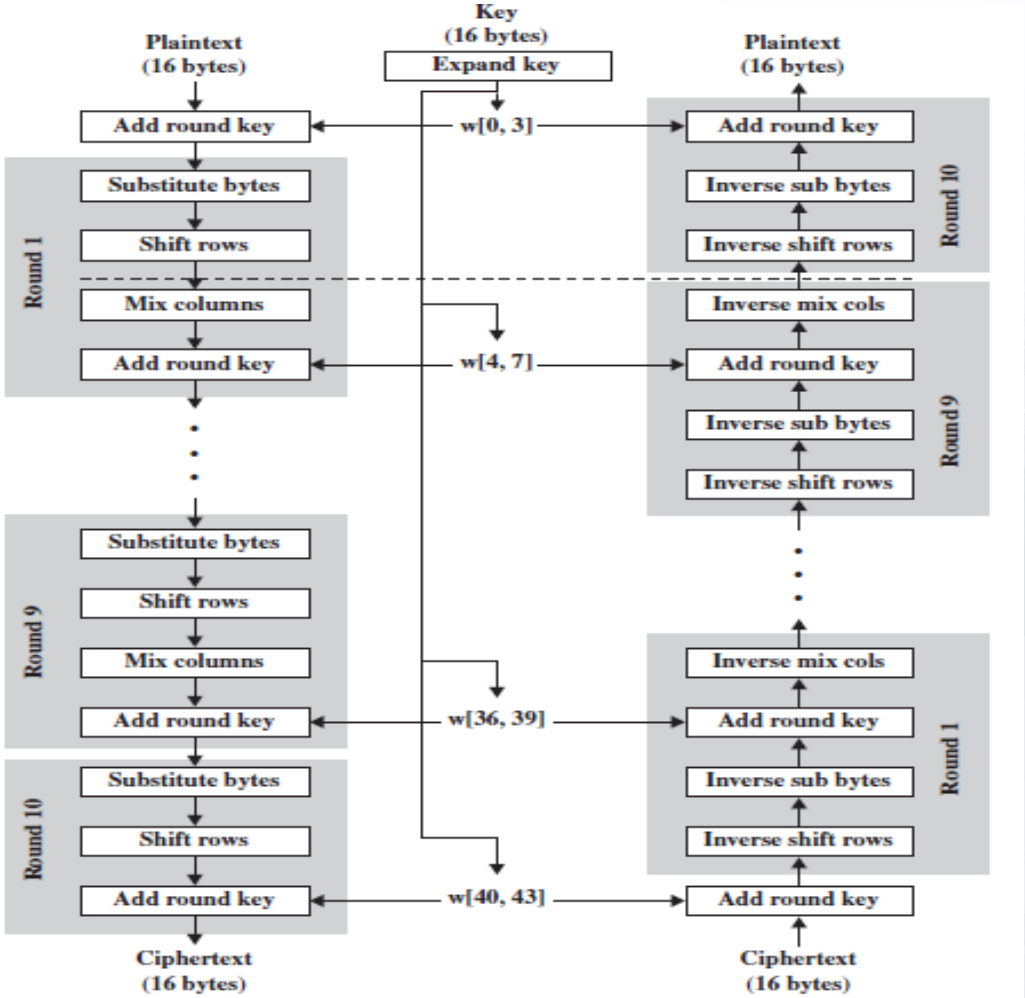


(a) Input, state array, and output

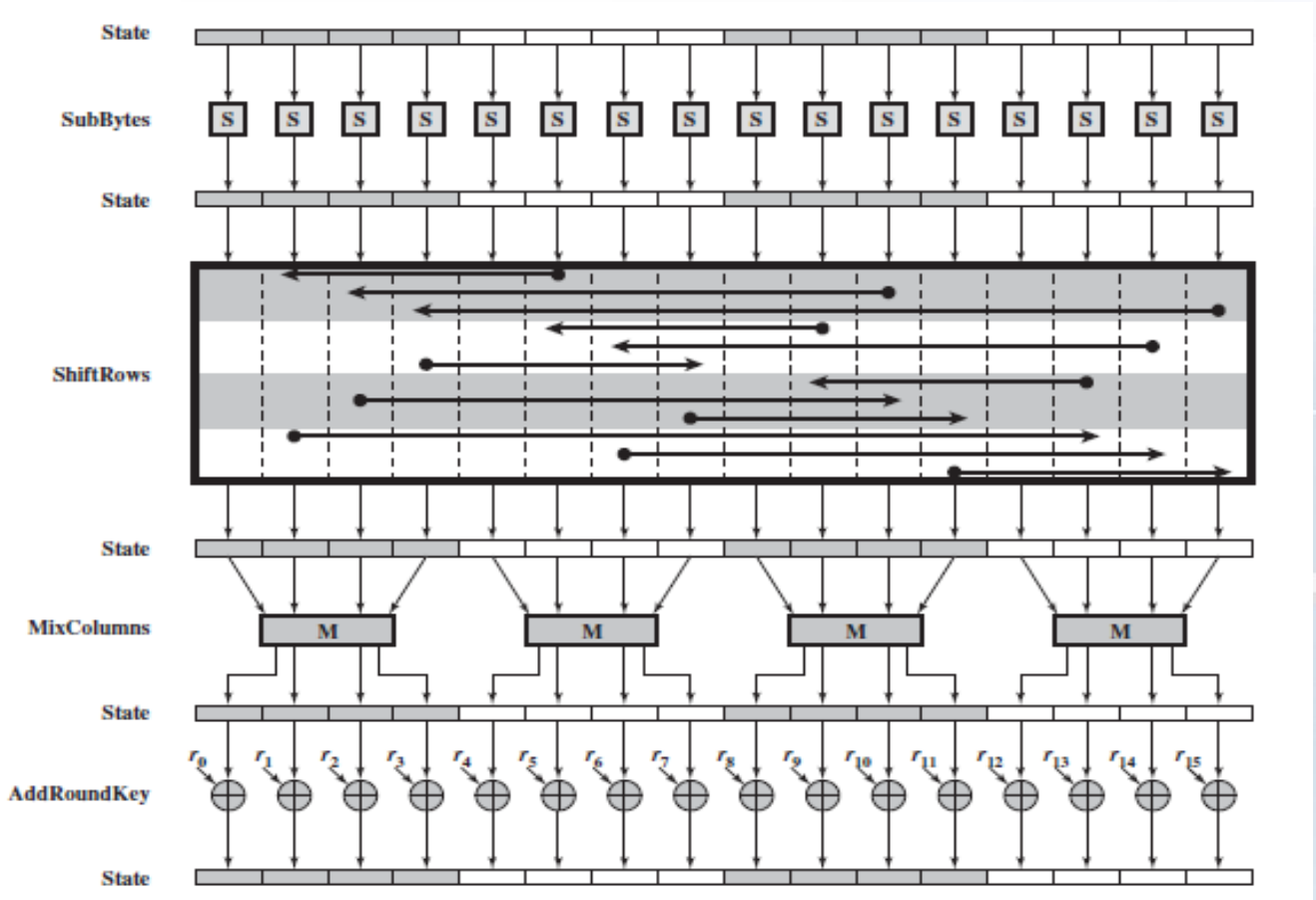
(b) Key and expanded key

Key Size (words/bytes/bits)	4/16/128	6/24/192	8/32/256
Plaintext Block Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Number of Rounds	10	12	14
Round Key Size (words/bytes/bits)	4/16/128	4/16/128	4/16/128
Expanded Key Size (words/bytes)	44/176	52/208	60/240

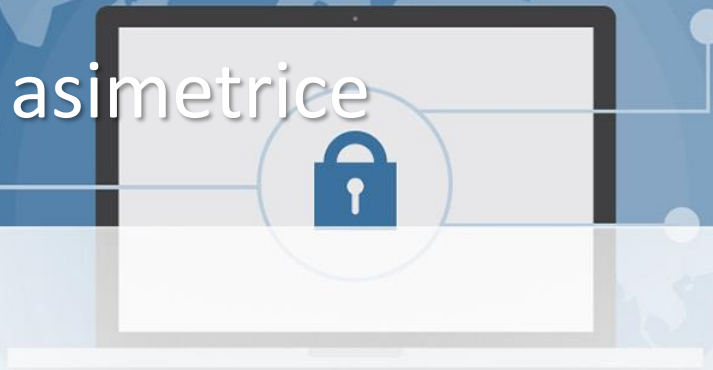
Criptare/ Decriptare AES



Runda AES


State
SubBytes
S
State
ShiftRows
State
MixColumns
M
State
AddRoundKey
State

Sisteme criptografice asimetrice



- Tehnici
- Cifruri cu cheie publică
- Sistemul de criptare RSA
- Criptografia cu chei publice
- Criptarea cu chei publice
- Semnătura digitală

Sisteme criptografice asimetrice

- Necesitate (probleme din sistemele simetrice)
  - Cheie unică
  - Distribuire cheie
  - Identificare (semnătura) electronică
- Criptografia asimetrică
  - O cheie pentru criptare
  - Altă cheie, diferită dar legată de prima, la decriptare
- Criptografia cu chei publice
- RSA (schema Rivest-Shamir-Adleman)

Sisteme criptografice Asimetrice

- Clasificare
  - Criptare / decriptare

    Expeditorul criptează un mesaj cu cheia publică a destinatarului
  - Semnătura digitală

    Expeditorul "semnează" un mesaj cu cheia sa privată. Semnarea este realizată printr-un algoritm criptografic aplicat mesajului sau unui mic bloc de date, care este o funcție a mesajului.
  - Schimb de cheie

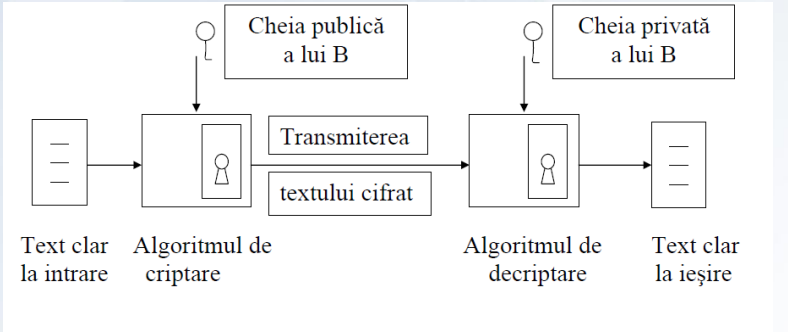
    Două entități pot să coopereze pentru a face schimb de cheie de sesiune. Mai multe diferit abordări sunt posibile, care implică cheia/cheile privată(e) ale uneia sau ale ambelor părți.

Criptografia cu chei publice - componente

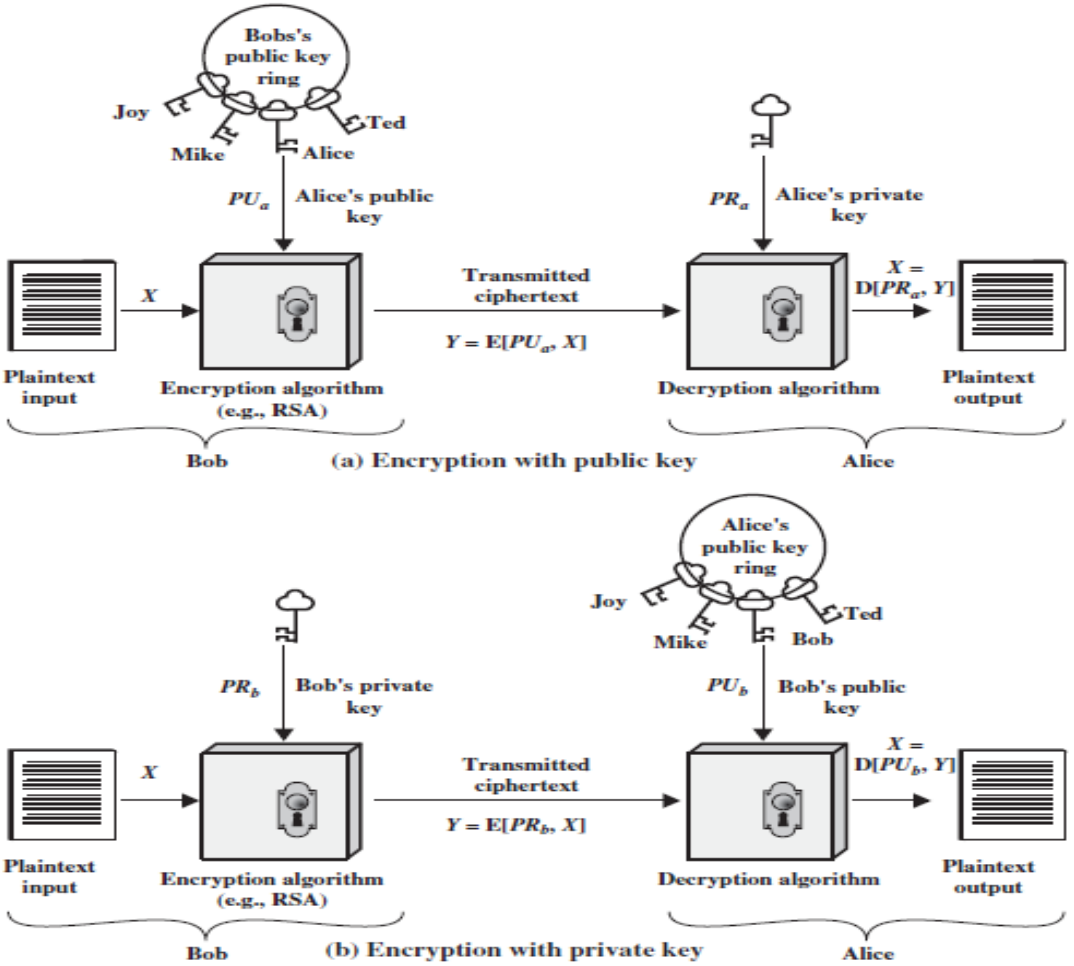
- O schemă de criptare cu chei publice conţine următoarele elemente:
  - Textul clar
    Acesta este un mesaj sau date de intrare pentru algoritmul de criptare.
  - Algoritmul de criptare
    Transformă textul clar în text cifrat.
  - Cheia publică şi cheia privată:
    Este o pereche de chei, una utilizată pentru criptare (cea publică) şi cealaltă pentru decriptare (cea privată).
  - Textul cifrat
    Textul produs în urma algoritmului de criptare. Pentru un mesaj dat, două chei diferite vor produce două texte cifrate diferite.
  - Algoritmul de decriptare
    Decriptează textul cifrat, în urma căruia rezultă textul clar.

Criptarea cu chei publice - principii

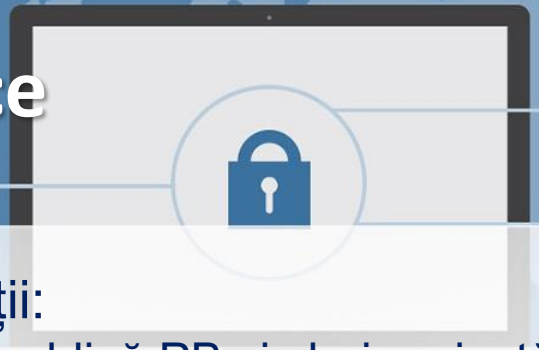
- Fiecare utilizator
  - generează o pereche de chei pentru criptarea și decriptarea de mesaje.
  - plasează una din cele două chei într-un registru public (cheia publică),
  - cheia pereche este menținută privată,
  - menține o colecție de chei publice obținute de la alții.
- Schimb de mesaje
  - Dacă A dorește să trimită un mesaj confidențial la B, A cripteaza mesajul folosind cheia publică a lui B
  - Când B primește mesajul, decriptează folosind cheia sa privată,
  - Nici un alt destinatar nu poate decripta mesajul, deoarece numai B știe propria cheie privată.



cheie publică/privată



Criptarea cu chei publice - condiții



Sunt respectate următoarele condiții:

- 1. B poate uşor să genereze cheia publică PB şi cheia privată SB.
- 2. Emitătorul A, ştiind cheia publică a lui B şi mesajul clar M, poate să genereze textul cifrat corespunzător:
- $C = E^{PB}(M)$
- 3. Receptorul B poate uşor să decripteze textul cifrat C:
- $M = D^{SB}(C) = D^{SB}(E^{PB}(M))$
- 4. Un atacator care ştie PB nu poate să determine cheia privată SB
- 5. Un atacator care ştie cheia publică PB şi textul cifrat C nu poate să determine mesajul original M
- 6. Are loc următoarea relație:
- $M = D^{SB}(E^{PB}(M)) = D^{PB}(E^{SB}(M))$.

Criptarea cu chei publice – Operații

- Operațiile criptografice
  - Secretizare

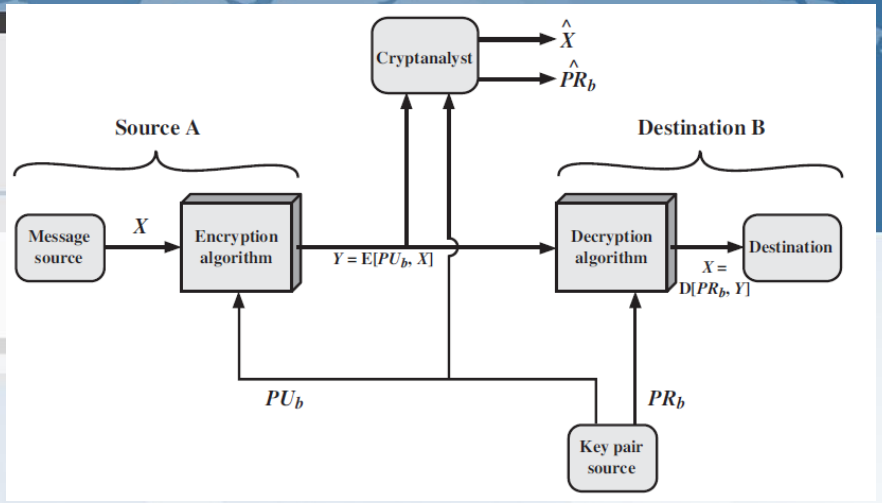
$$Y = \mathrm{E}(PU_b, X)$$

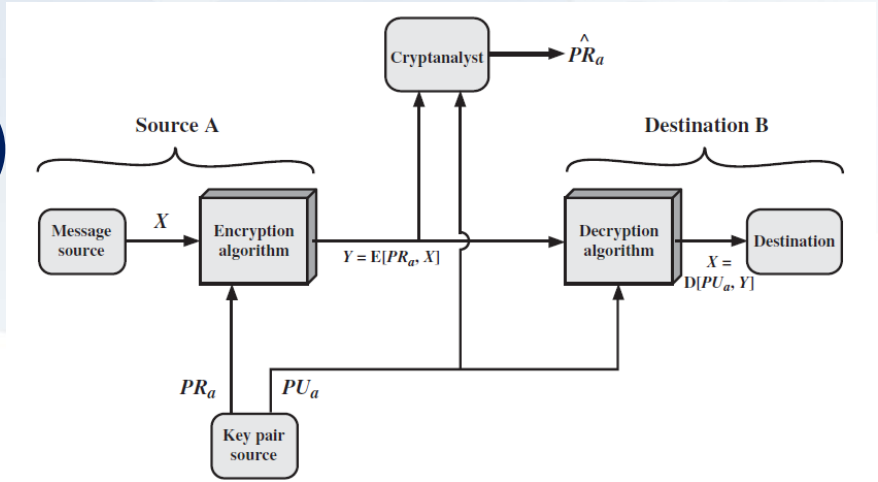
$$X = \mathrm{D}(PR_b, Y)$$

  - Autentificare (certificare) (semnătură electronică)

$$Y = \mathrm{E}(PR_a, X)$$

$$X = \mathrm{D}(PU_a, Y)$$



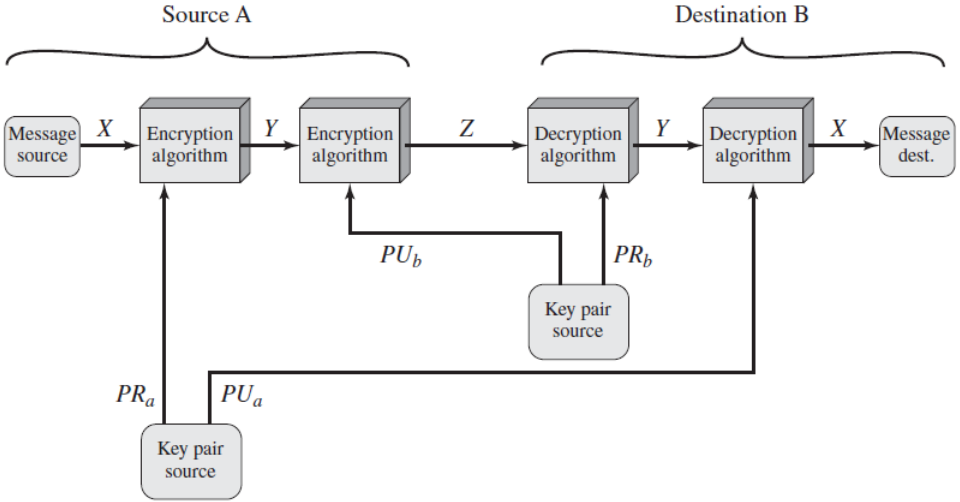


Criptarea cu chei publice – Operații (2)

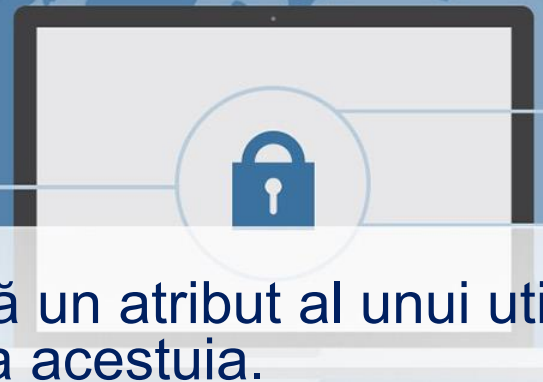
- Operațiile criptografice combinate
  - Secretizare și autentificare

$$Z = \mathrm{E}(PU_b, \mathrm{E}(PR_a, X))$$

$$X = \mathrm{D}(PU_a, \mathrm{D}(PR_b, Z))$$

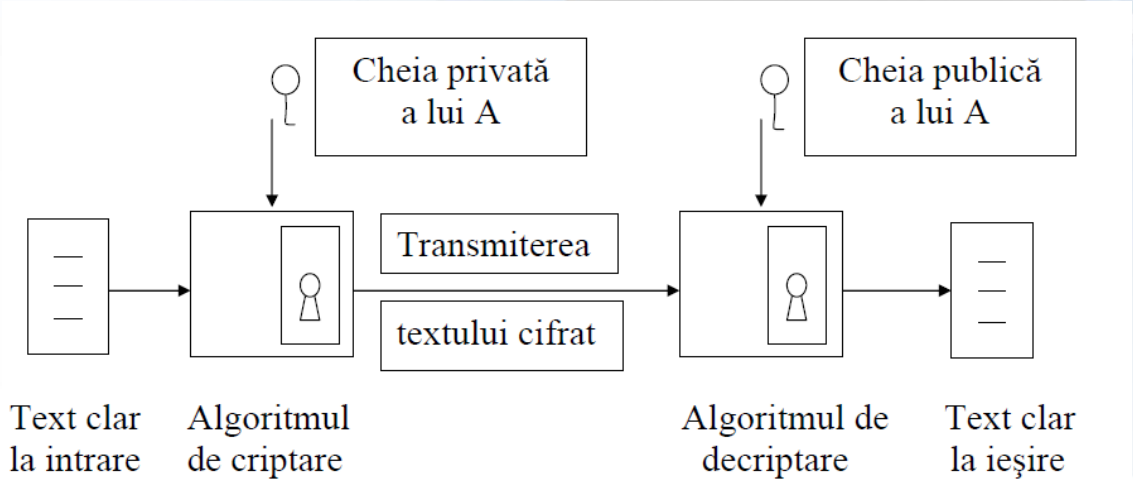


Semnătura digitală



- Semnătura digitală reprezintă un atribut al unui utilizator, fiind folosită pentru recunoaşterea acestuia.
- Fie B un receptor de mesaj semnat de A.
- Semnătura lui A trebuie să satisfacă următoarele proprietăţi:
  - Utilizatorul B să fie capabil să valideze semnătura lui A
  - Să fie imposibil pentru oricine, inclusiv B, să falsifice semnătura lui A
  - În cazul în care A nu recunoaşte semnătura unui mesaj M, trebuie să existe un „judecător” care să poată rezolva disputa dintre A şi B.

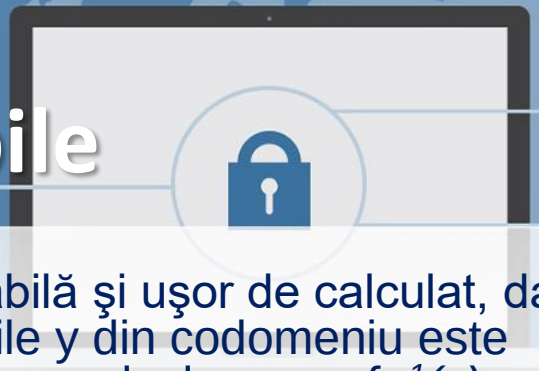
Semnătura digitală



criptare cu chei publice - Aplicații

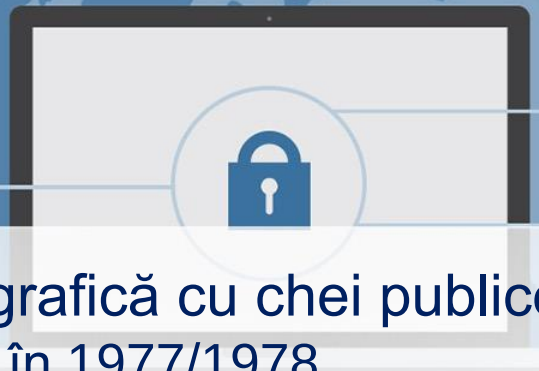
Algoritm	Criptare/Decriptare	Semnătură digitală	Distribuția cheilor
RSA	DA	DA	DA
Diffie-Hellman	NU	NU	DA
DSS	NU	DA	NU
Algoritmi bazați pe curbe eliptice	DA	DA	DA

Funcții greu inversabile



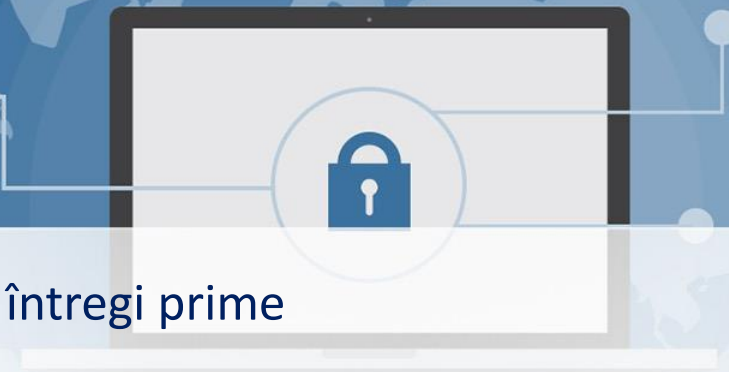
- O funcție este greu inversabilă şi uşor de calculat, dar pentru aproape toate valorile y din codomeniu este imposibil computațional să se calculeze $x = f^{-1}(y)$.
- Cu alte cuvinte este imposibil computațional să se calculeze f^{-1} dacă se dispune de o descriere completă a lui f.
- O funcție greu inversabilă se spune că este cu trapă atunci când f^{-1} este uşor de calculat numai dacă se dispune de o informație trapă.
- Necunoaşterea acestei informații face ca funcția să fie greu inversabilă.
- O astfel de pereche de funcții (f, f^{-1}) poate constitui perechea (E,D) a unui criptosistem cu chei publice.

Criptosistemul RSA



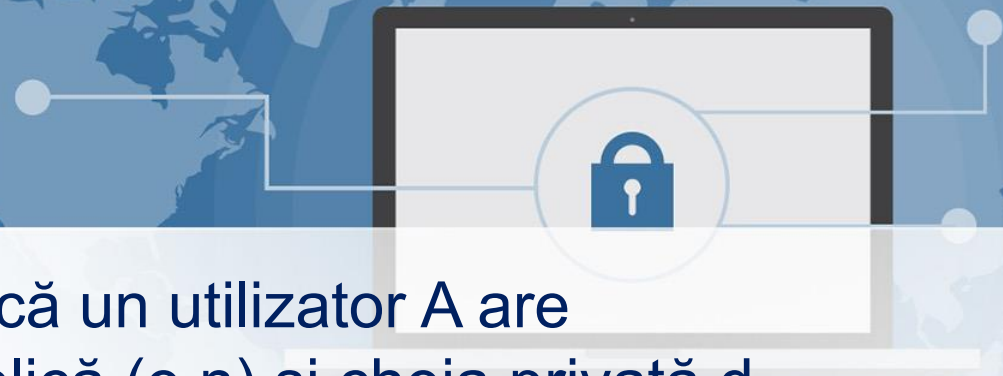
- Prima schemă criptografică cu chei publice
  - dezvoltată/publicată în 1977/1978
  - de Ron Rivest, Adi Shamir şi Len Adleman de la MIT.
- Schema Rivest-Shamir-Adleman (RSA)
  - cea mai răspândită şi implementată schemă din lume
  - algoritm criptografic cu chei publice
  - textul clar și cel cifrat sunt numere între 0 și n-1, *n* fiind ales (de obicei 1024 biți ($n<2^{1024}$) sau 309 cifre zecimale)
  - algoritm de criptare pe blocuri (mesajul este împărțit în blocuri, care sunt cifrate pe rând)

RSA – generarea cheilor



- 1. Se selectează două numere întregi prime
  p şi q.
- 2. Se calculează produsul
  n=p*q.
- 3. Se calculează indicatorul lui Euler
  $\Phi(n)=(p-1)*(q-1)$
- 4. Se selectează un număr întreg *e,* astfel încât
  c.m.m.d.c. $(\Phi(n),e)=1$, $1<e<\Phi(n)$.
- 5. Se calculează *d* astfel încât
  $d = e^{-1} \bmod \Phi(n)$.
- 6. Cheia publică este *(e,n),* iar cheia privată este (*d,n).*

RSA – criptare



- Presupunem că un utilizator A are
  cheia publică (e,n) şi cheia privată d.
- Utilizatorul B criptează mesajul M pentru a fi transmis la A astfel:
  - 1. Obține cheia publică (e,n) a lui A.
  - 2. Transformă mesajul ce va fi criptat într-un număr întreg M în intervalul [0,n-1].
  - 3. Calculează $C = M^e \pmod n$.
  - 4. Trimite textul cifrat C la utilizatorul A.

RSA – decriptare

- Pentru a determina textul clar M din textul cifrat C,
  - utilizatorul A calculează:

    $M = C^d \pmod{n}$.
- Important
  - Numai utilizatorul A cunoaște cheia privată d.

Algoritmul RSA

Key Generation A

Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calcuate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption by B with A Public Key

Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption by A with A Public Key

Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Exemplu RSA

Generare cheie

$p = 17$ and $q = 11$.

$n = pq = 17 \times 11 = 187$.

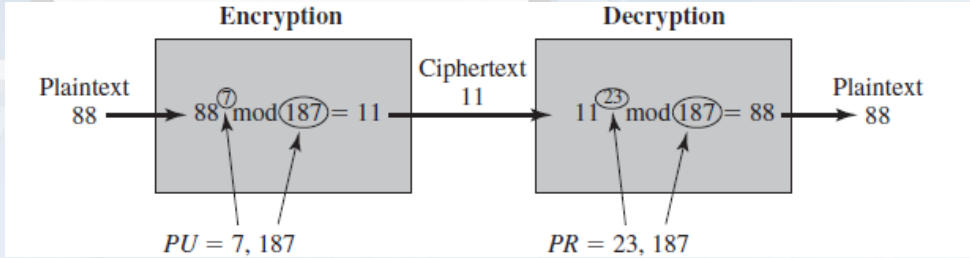
$\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$.

$e = 7$

$de \equiv 1 \pmod{160}$ $\quad d = 23$

$PU = \{7, 187\}$

$PR = \{23, 187\}$



Criptare

$$88^7 \bmod 187 = [(88^4 \bmod 187) \times (88^2 \bmod 187) \times (88^1 \bmod 187)] \bmod 187$$

$88^1 \bmod 187 = 88$

$88^2 \bmod 187 = 7744 \bmod 187 = 77$

$88^4 \bmod 187 = 59{,}969{,}536 \bmod 187 = 132$

$88^7 \bmod 187 = (88 \times 77 \times 132) \bmod 187 = 894{,}432 \bmod 187 = 11$

Decriptare

$$11^{23} \bmod 187 = [(11^1 \bmod 187) \times (11^2 \bmod 187) \times (11^4 \bmod 187) \times (11^8 \bmod 187) \times (11^8 \bmod 187)] \bmod 187$$

$11^1 \bmod 187 = 11$

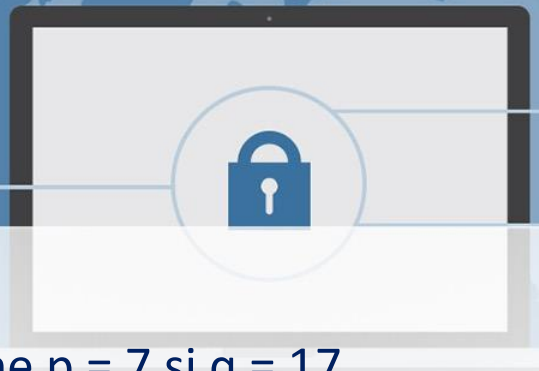
$11^2 \bmod 187 = 121$

$11^4 \bmod 187 = 14{,}641 \bmod 187 = 55$

$11^8 \bmod 187 = 214{,}358{,}881 \bmod 187 = 33$

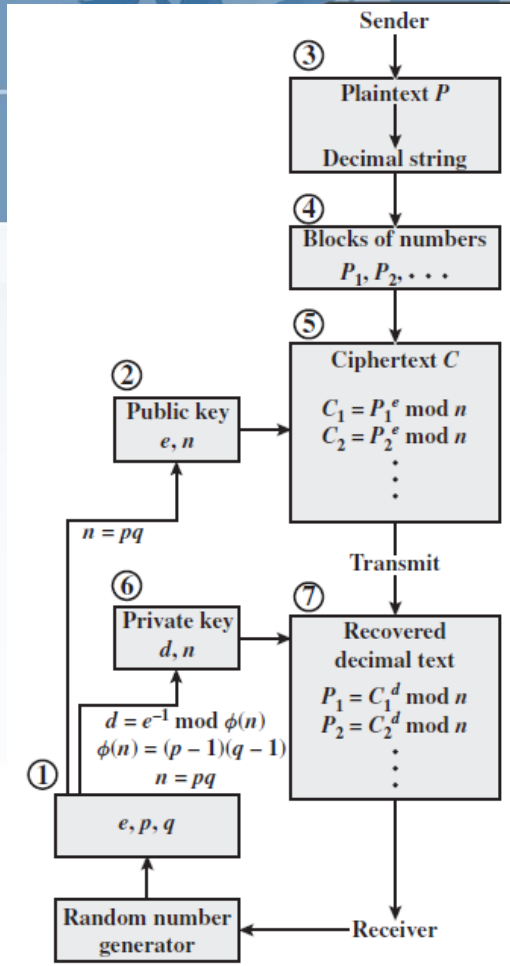
$11^{23} \bmod 187 = (11 \times 121 \times 55 \times 33 \times 33) \bmod 187 = 79{,}720{,}245 \bmod 187 = 88$

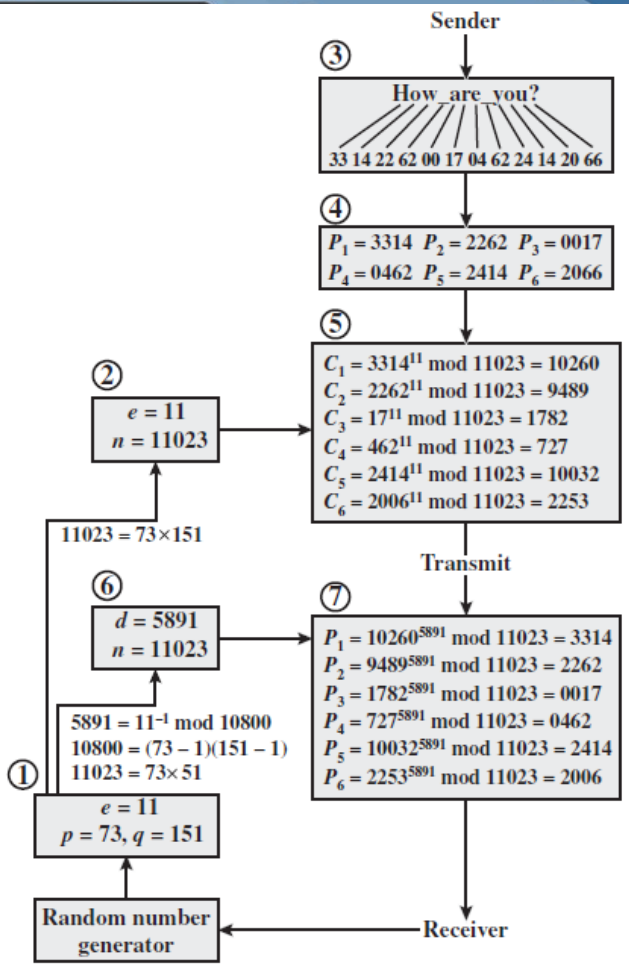
RSA - exemplu



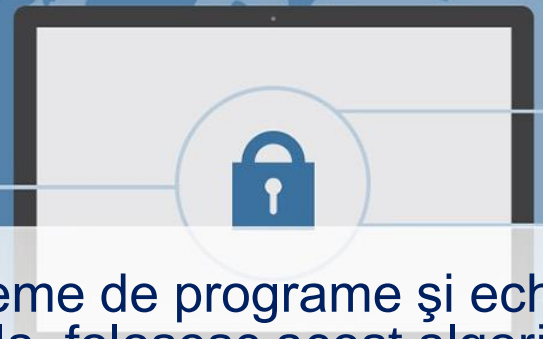
- Se generează mai întâi cheile:
- 1. Se selectează două numere prime p = 7 şi q = 17.
- 2. Se calculează n = p*q = 7*17 = 119.
- 3. Se calculează Φ(n) = (p-1)*(q-1) = 96.
- 4. Se alege e a. î. e este relativ prim cu Φ(n) = 96. În acest caz e = 5.
- 5. Se determină d astfel încât d*e = 1 mod 96 şi d<96. Avem d = 77, deoarece 77*5 = 385 = 4*96+1.
- 6. Cheia publică este (5,119), iar cheia privată este 77.
  - Se consideră că textul clar este M =19.
  - Textul criptat va fi C = 19^5 mod 119 = 2476099 mod 119 = 66.
  - Pentru decriptare se calculează 66^{77} mod 119 = 19 mod 119.

RSA– Procesare blocuri



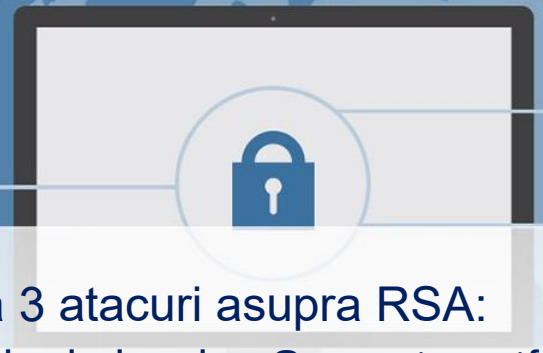


RSA - Atacuri



- Firme producătoare de sisteme de programe şi echipamente, ca Novell, DEC, Lotus, Motorola, folosesc acest algoritm.
- Instituții importante (Departamentul Apărării din SUA, Boeing, rețeaua bancară internațională SWIFT) folosesc acest algoritm pentru protejarea şi autentificarea datelor, parolelor, fişierelor, documentelor memorate sau transmise prin rețele.
- Există trei tipuri de atacuri asupra algoritmului RSA:
  - Încercarea tuturor cheilor private posibile.
  - Factorizarea numărului n în factori primi p şi q.
  - Aceste atacuri depind de timpul de execuție a alg. de decriptare

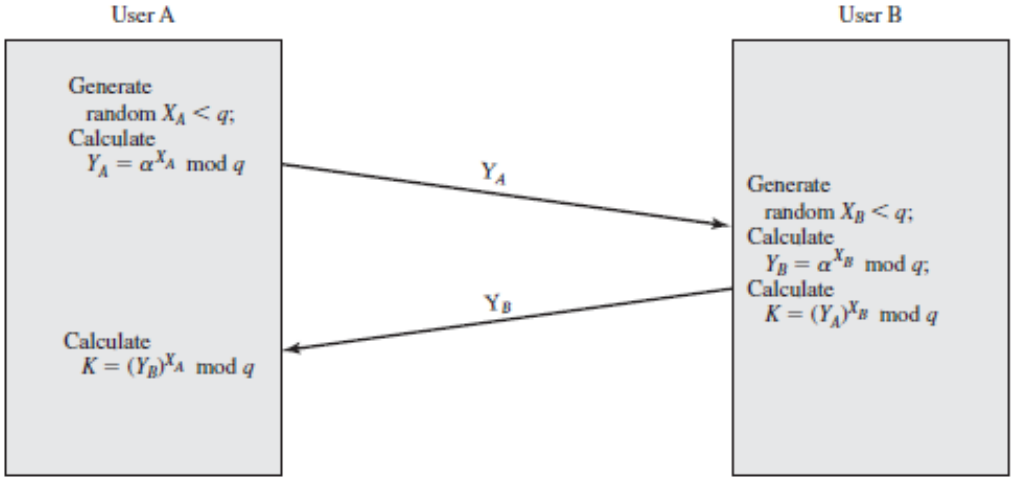
RSA - atacuri



- Din punct de vedere matematic, există 3 atacuri asupra RSA:
  - 1. Factorizarea numărului n în factori primi p şi q. Se poate astfel determina $\Phi(n) = (p-1)*(q-1)$, iar apoi $d = e^{-1} \pmod{\Phi(n)}$.
  - 2. Determinarea lui $\Phi(n)$ direct, fără a determina mai întâi p şi q. Şi în acest caz se poate determina apoi $d = e^{-1} \pmod{\Phi(n)}$.
  - 3. Determinarea lui d în mod direct, fără a determina mai întâi $\Phi(n)$.
- Determinarea lui $\Phi(n)$ este echivalent cu factorizarea numărului n, iar determinarea lui d (ştiind doar pe e şi n) se face într-un timp tot aşa de mare ca şi factorizarea lui n.
- Securitatea RSA se bazează pe dificultatea factorizării unui număr întreg în factori primi.
- RSA cu lungimea cheii de 1024 biți (aproximativ 300 cifre) este considerat destul de puternic pentru aplicațiile actuale.

Alte sisteme cu cheie publică

- Sistem de distribuție chei Diffie-Hellman



- Criptosistemul ElGamal
- Sisteme bazate pe curbe eliptice

Algoritm Diffie-Hellman

Global Public Elements

q	prime number
α	$\alpha < q$ and α a primitive root of q

User A Key Generation

Select private X_A	$X_A < q$
Calculate public Y_A	$Y_A = \alpha^{XA} \bmod q$

User B Key Generation

Select private X_B	$X_B < q$
Calculate public Y_B	$Y_B = \alpha^{XB} \bmod q$

Calculation of Secret Key by User A

$$K = (Y_B)^{XA} \bmod q$$

Calculation of Secret Key by User B

$$K = (Y_A)^{XB} \bmod q$$

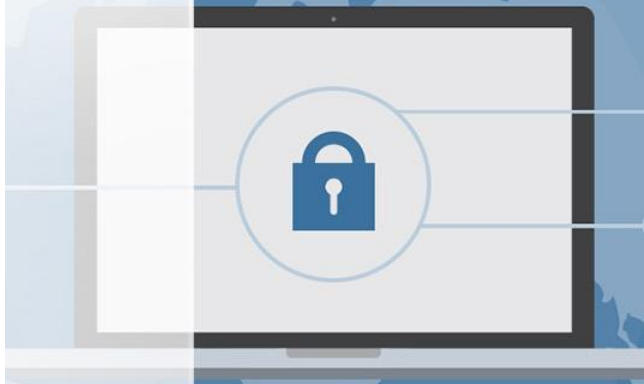
Criptosistemul ElGamal

Global Public Elements	
q	prime number
α	$\alpha < q$ and α a primitive root of q

Key Generation by Alice	
Select private X_A	$X_A < q - 1$
Calculate Y_A	$Y_A = \alpha^{XA} \bmod q$
Public key	$PU = \{q, \alpha, Y_A\}$
Private key	X_A

Encryption by Bob with Alice's Public Key	
Plaintext:	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Ciphertext:	(C_1, C_2)

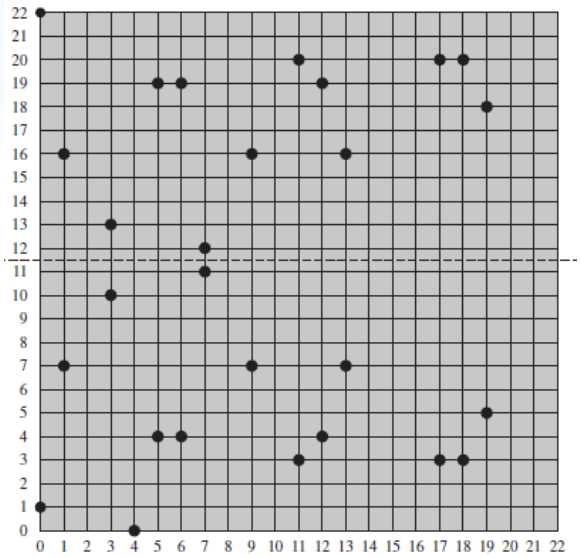
Decryption by Alice with Alice's Private Key	
Ciphertext:	(C_1, C_2)
Calculate K	$K = (C_1)^{XA} \bmod q$
Plaintext:	$M = (C_2 K^{-1}) \bmod q$

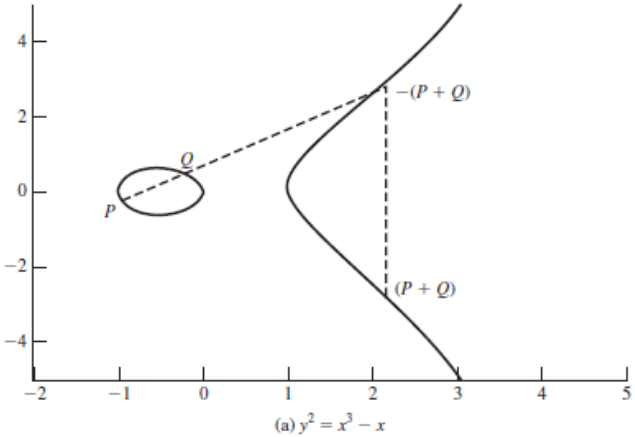


Sisteme bazate pe curbe eliptice - ECC

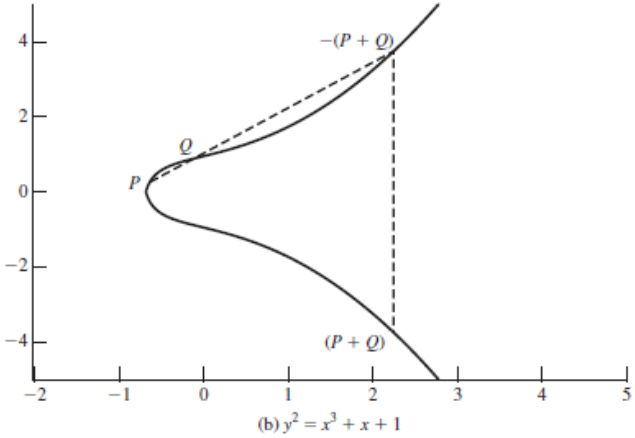
- Puncte pe curbe eliptice

(0, 1)	(6, 4)	(12, 19)
(0, 22)	(6, 19)	(13, 7)
(1, 7)	(7, 11)	(13, 16)
(1, 16)	(7, 12)	(17, 3)
(3, 10)	(9, 7)	(17, 20)
(3, 13)	(9, 16)	(18, 3)
(4, 0)	(11, 3)	(18, 20)
(5, 4)	(11, 20)	(19, 5)
(5, 19)	(12, 4)	(19, 18)





(a) $y^2 = x^3 - x$



(b) $y^2 = x^3 + x + 1$

ECC Diffie-Hellman

Global Public Elements

$E_q(a, b)$	elliptic curve with parameters a, b, and q, where q is a prime or an integer of the form 2^m
G	point on elliptic curve whose order is large value n

User A Key Generation

Select private n_A	$n_A < n$
Calculate public P_A	$P_A = n_A \times G$

User B Key Generation

Select private n_B	$n_B < n$
Calculate public P_B	$P_B = n_B \times G$

Calculation of Secret Key by User A

$K = n_A \times P_B$

Calculation of Secret Key by User B

$K = n_B \times P_A$

Lungime cheie

Symmetric Scheme (key size in bits)	ECC-Based Scheme (size of n in bits)	RSA/DSA (modulus size in bits)
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360