01.03.2016

S1 Pag1

S1

CRIPTO

① Sist. cavalerilor de Malta

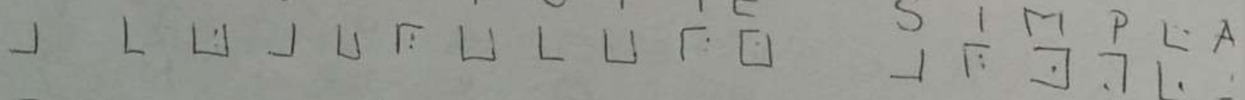
A:	B:	C:
D:	E:	F:
G:	H:	I:

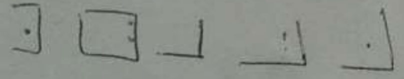
J.	K.	L.
M.	N.	O.
P.	Q.	R.

S	T	U
V	W	X
Y	Z	

a) SUBSTITUȚIE SIMPLĂ

S U B S T I T U T I E SIMPLA



b) 

M E S A J

c) Nr. chei = 1

② Sistemul Polybius (i = J)

a) S U B S T I T U T I E

43 45 15 43 44 32 44 45 44 32, 23

linie coloană

cheia = POL

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

cheia

	1	2	3	4	5
1	P	O	L	A	B
2	C	D	E	F	G
3	H	I/J	K	M	N
4	Q	R	S	T	U
5	V	W	X	Y	Z

S1 Pag 2

b) 21 32 24 42 45

e i F R U

c) nr. chei : 25!

③ Cezar cu cheie

a) C R I P T O G R A F I E , k=4

F V M T X S K V E J M I

A	B	C	D	E	F	G	H	I	J	K	L
E	F	G	H	I	J	K	L	M	N	O	P

M	N	O	P	Q	R	S	T
Q	R	S	T	U	V	W	X

b) ECFDEPO ALCEJ , k = 11

TRUSTED PARTY

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

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

c) nr chei posibile = 26

④ sist. afin

$k = (k_1, k_2)$

$Enc^k (m) = (k_1 m + k_2)(\text{mod } 26)$

a) T E X T $k = (3,5)$
K R W K

0	1	2	3	4	5	6	7	8	9
A	B	C	D	E	F	G	H	I	J
10	11	12	13	14	15	16	17	18	19
K	L	M	N	O	P	Q	R	S	T
20	21	22	23	24	25				
U	V	W	X	Y	Z				

$T \to (\overset{k_1}{3} \cdot \overset{\overset{T}{\|}}{\overset{m}{19}} + \overset{k_2}{5}) \text{mod } 26 = 62 \% 26 = 10$

$E \to (3 \cdot 4 + 5) \% 26 = 17$

$X \to (3 \cdot 23 + 5) \% 26 = 74 \% 26 = 22$

b) $k_1 m + k_2 = c$, $m = \frac{c-5}{3} \% 26 =$

$3m + 5 = c$

$= ((c-5) * 9) \% 26$

?? : $\frac{1}{3}(\text{mod } 26) \cdot 3 =$
$= 1(\text{mod } 26)$
$\underline{9}$

P R H F G , $k = (3,5)$

$\to ((15-5)*9) \% 26$

$P \to 90 \% 26 =$ M

R → E
H → S
F → A
G → Z

c) nr. de chei

26^2

Sisteme de substituție simplă

5) a) WEB DESIGN
criptat: VSR WSPDAJ
folosind BROWSER

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

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

b) ⇒ PUBLIC KEY

c) nr. chei: 26!

Sisteme de transpoziție

6) STANDARDUL DE CRIPTARE

$\sigma = (\overset{1}{2}, \overset{2}{3}, \overset{3}{1})$

	1	2	3
1	S	T	A
2	N	D	A
3	R	D	U
4	L	D	E
	C	R	I
	P	T	A
	D	E	

← criptat

C R I
P T A
R E

TAS
DAN
DUR
DEL
RIC
TAP
ER

S1 Pag 1

S1 Pag 5

[TASPANDURDEL RICTAPER] linii

mesajul criptat scris pe coloane:

TDDARTEAAUEISNRLCPR coloane

h) STCME TAEAE NER

$\sigma - (\overset{1}{1}, \overset{2}{2}, \overset{3}{3})$

S T E
T A N
C E L
M A R
E

S E A R
T T E
C A N
M E E

→ STEFAN CEL MARE

7 a) Sistem mixt
Cezar + permutare

orice ordine (transp. & perm.)

S i S T E M M i X T

Sistem Cezar + perm.
k = 3 ; σ(2,3,1)

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

→ după Cezar: VLVWHPPLAW

S1 Pag 6

σ(2,3,1)
1,2,3

1	2	3
V	L	V
W	H	P
P	L	A
W		

→ L V V
H P W
L A P
W

~~LHLWPAVWPW~~

↗ LHLWVPAVWP

b) CPKQCG ZGTVTK GOERIH

σ(3,2,1) , K=2

→ Cezar ~~ARGEAC~~
→ ANIOAE XERTRI EMCPGT

1	2	3
A	X	E
N	E	M
I	R	C
O	T	P
A	R	G
E	I	T

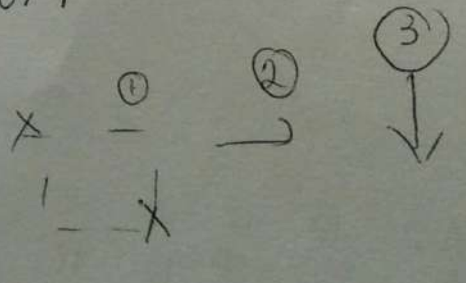
↙σ

→ EXAMEN CRIPTOGRAFIE
decriptat

(8) PLAY FAIR (I=J) Nr. de chei : $\frac{25!}{5^2}$

a) TH|E CI|RC|LEX , cheia = ALBUM
PO|T DK|DA|KB
Q

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



BA LX LX
UL

5×5

<parola>
restul alfabetului
fără literele din
<parola>

b) PIGOY QLETY AEYLQ YSFWN S1 Pag7

cheie · CRYPTOOL

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

THE ART OF PROGRAMXMING

15.03.2016

CRIPTO

① OTP

$c = m \oplus k$

$m = c \oplus k$

a) $dec_k(enc_k(m)) = k \oplus (k \oplus m) = m$

└> Arătați că un sistem de criptare e corect

b) ! - nu am putea utiliza cheia

& - nu e reversibil

~~ex. $c = 1$~~

~~$k = 1$~~

~~$\underbrace{c \wedge k}_{m} = 1$~~

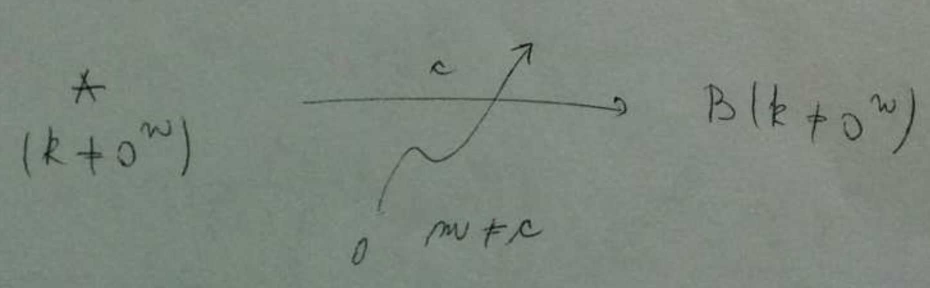
$k = 1$ | același mesaj criptat ($\vee$)

$m = 0$ sau 1 |

$k = 0$ | mesaj criptat 0 ($\wedge$)

mesaj clar 0 sau 1 |

② $Pr[M = m \mid C = c] = Pr[M = m] \quad \forall m, \forall c$



a) Știe că nu e c, deci NU e perfect sigur

Superman

S2 Pag 2

lol

③ OTP

Tot 1 GB

④ OTP

(m, c)

a) Aflăm $k = m \oplus c$

b) (m, c)

(m', c')

XOR	0	1
0	0	1
1	1	0

⑤ $\Pr[M = m_1 \mid C = c] = \Pr[M = m_2 \mid C = c]$

$m_1, m_2 \in \mathcal{M}$

NU!

$$\underset{\displaystyle \Pr[m = m_1]}{\underset{\shortparallel}{\Pr[M = m_1 \mid C = c]}} = \underset{\displaystyle \Pr[m = m_2]}{\underset{\shortparallel}{\Pr[M = m_2 \mid C = c]}}$$

⑥ NU!

$c = m \parallel k$

⑦ PPT $\mathcal{A}$

$\exists\, n_\varepsilon,\ \forall\, n > n_\varepsilon,\ f(n) < \frac{1}{p(n)},$

$\forall\, p(n)$

$\boxed{p(n)\cdot\varepsilon \not> 1}$

a) $f(n) = \frac{1}{n^{100}} > \frac{1}{n^{101}}$ → NU!

b) $f(n) = \frac{1}{3^n}$ DA!

c) $f(n) = \begin{cases} \frac{1}{n^{100}}, & n \text{ par} \\ \frac{1}{3^n}, & n \text{ impar} \end{cases}$ nu e neglijabilă ⟩ nu e neglijabilă

d) $f(n) = \frac{1}{2} + negl(n)$ Nu e neglijabilă

e) $f(n) = \frac{p(n)}{2^n}$ DA! Pp. $\frac{p(n)}{2^n} > \frac{1}{p'(n)}$, $p(n)p'(n) > 2^n$!

f) $f(n) = \frac{1}{6}$ nu e neglijabilă pt. că e constantă

(8)

$$\begin{tikzcd} {} \arrow[d, "k"] \\ \boxed{PRG} \arrow[d] \\ G(k) \end{tikzcd}$$

- $G(k) > k$
- să pară random

$G : \{0,1\}^k \to \{0,1\}^k$, $k < n$

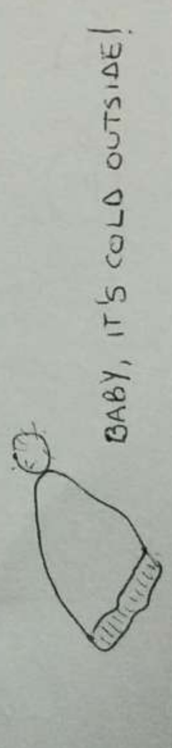
a) $msb(G(s)) = 1$, $\forall s$

b) $msb(G(s)) = 1$ cu prob. $\frac{1}{n^{100}}$

c) $G(s) = G_0(s) \| G_1(s) \| G_2(s)$, unde

$|G_0(s)| = |G_1(s)| = |G_2(s)|$,

$G \ (s) = G \ (s) \oplus G \ (s)$



d) $G(s) = G_0(s) \| G_1(s)$, unde $G_0(s) = F(G_1(s))$,

F cunoscută

a) NU! - pt că nu e pseudoaleator

b) $\boxed{A}$ PPT

↳ output $\begin{cases} r \xleftarrow{R} \{0,1\}^n \\ G \end{cases}$ $k < n$

A vede output: zice PRG dacă msb(output) = 1

zice random dacă msb(output) = 0

↑ rep. pt s. dif

NU! - diferă cu o probabilitate neneglijabilă $\left(\frac{1}{n^{100}}\right)$

e PRG

c) NU

d) NU

(10) F' PRF

$\not\!\overline{\qquad\qquad}$

F PRF?

$$F_k(x) = \begin{cases} F'_k(x) & , x \text{ par} \\ F'_k(x+1) & , x \text{ impar} \end{cases}$$

$F_k(1) = F'_k(2)$ NU e PRF

$F_k(2) = F'_k(2)$

(11) $F \quad \mathcal{K} \times \mathcal{X} \rightarrow \{0, 1\}^{128}$ PRF

$$F'_k(x) = \begin{cases} 0^{128} & , x = 0 \\ F_k(x) & , x \neq 0 \end{cases}$$

Este F' PRF?

0^{128} - 0 peste tot pe 128 biți

NU!

- F' PRF

$F_k(x) = F'_k(x) \oplus 1^n$

ESTE PRF!

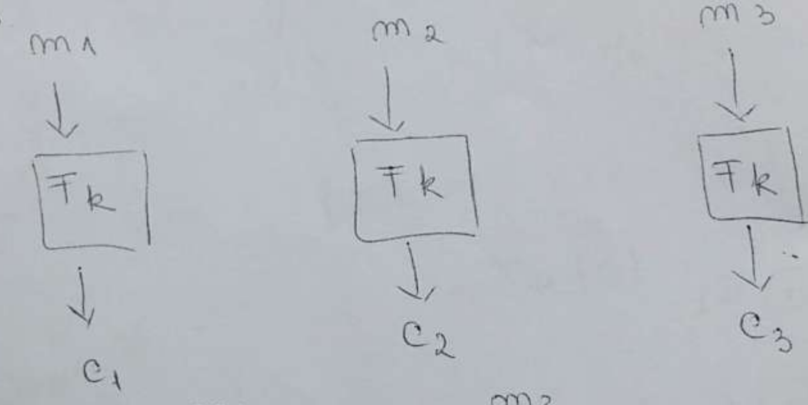
S3

29.03.2016 CRIPTO

Moduri de operare.

(1) moduri de operare ECB, CBC, OFB, CTR

ECB

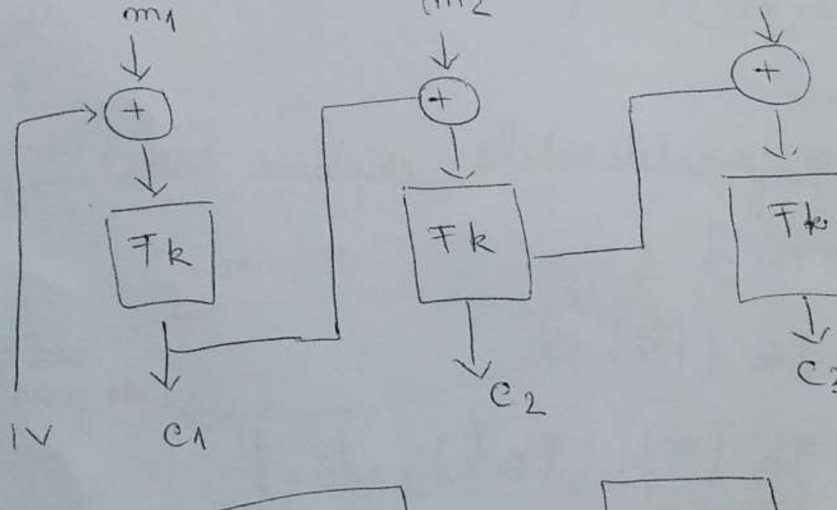


E paralelizabilă la cript. și decript

$c_1 = F_k(m_1)$

$m_1 = F_k^{-1}(c_1)$

CBC

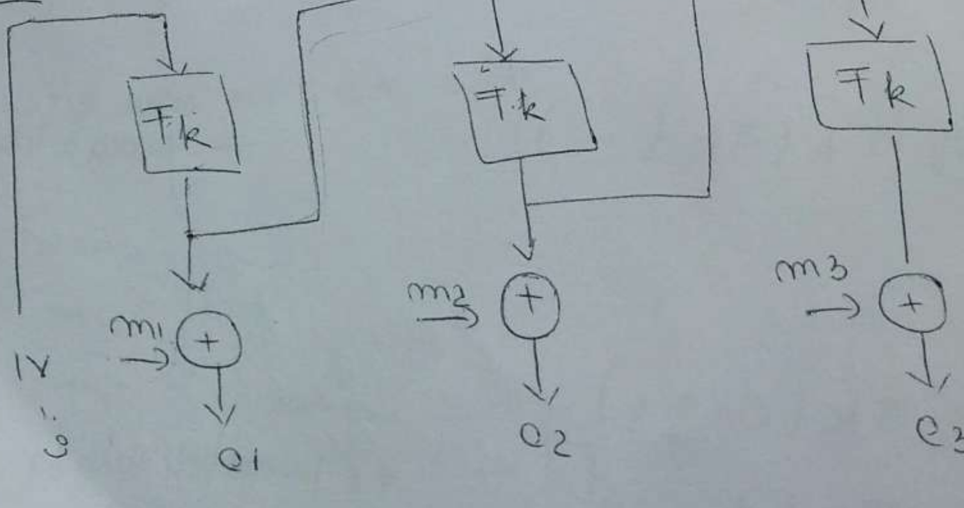


$c_0 = IV$ iv

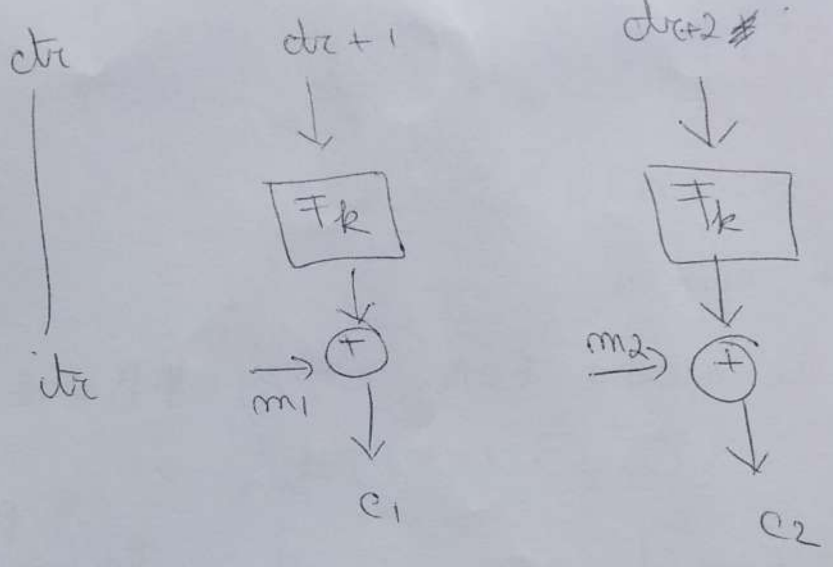
$c_1 = F_k(c_{i-1} \oplus m_1)$

$c_i = F_k(F_k(\dots(iv \oplus m_1))\dots))$

OFB



CTR



CBC

$m_3 = F_k^{-1}(c_3) \oplus c_2$

$m_i = F_k^{-1}(c_i) \oplus c_{i-1}$

~~Ambele sunt~~
Decriptarea e paralelizabilă, criptarea nu.

OFB

$c_1 = m_1 \oplus F_k(iv)$ → nu e paralelizabilă

$c_i = m_i \oplus F_k(F_k(F_k(\dots))\dots)$

decriptare:

$m_1 = c_i \oplus F_k(F_k(\dots))$ → nu e paralelizabi

CTR

$c_0 = ctr$

$c_i = m_i \oplus F_k(ctr + i)$ → nu e paralelizabilă

$m_i = c_1 \oplus F_k(ctr + i)$

01.03.2016

②	1	2	3	4	5
ECB	BANCA A	CONTUL CA	BANCA B	CONTUL CB	SUMA (EUR)

- aceeaşi bancă
- nu ştie cheia
- facem un transfer din contul lui în banca respectivă, vede care e contul şi înlocuieşte bucata criptată.

③ CBC

$$\begin{tikzcd} \mathcal{A} \arrow[r, bend left, "m_0, m_1"] & \mathcal{C} \arrow[l, bend left, "c = Enc_k(m_b)"] \end{tikzcd}$$

PPT ↓ $b' \in \{0,1\}$

$k \leftarrow \mathcal{K}$

$\mathcal{C}$ Selează $b \in \{0,1\}$

$$\begin{cases} b=0, \text{ criptează } m_0 \\ b=1, \text{ criptează } m_1 \end{cases}$$

$$\begin{tikzcd} \mathcal{A} \arrow[r, bend left, "m"] & \text{Oracol criptare } (k) \arrow[l, bend left, "c"] \end{tikzcd}$$

$\boxed{CPC}$

Schema sigură când avantajul $\mathcal{A} < \frac{1}{2} + negl(n)$

$$\begin{tikzcd} \mathcal{A} \arrow[r, bend left, "c' \neq c"] & \text{Oracol decriptare} \arrow[l, bend left, "m'"] \end{tikzcd}$$

$\boxed{CCA}$

01.03.2016

$m_0 = iv$

$m_1 = iv+1$. Dacă ar fi m_1 : $c_1 = iv+1$,

$F_k(iv+1 \oplus iv+2) = F_k(0))$

♡ zâmbește! Iulia o aude? >:)

. Dacă ar fi m_0 :

$iv, F_k(iv+1 \oplus iv)$

$m = iv+2 \Rightarrow iv+2, F_k(iv+2 \oplus iv+2) =$

$= F_k(0)$

trebuie să trimitem $m = iv+2$

$A \xrightarrow{m}$ Oracol

④
$$\begin{tikzcd} A \arrow[r, bend left, "m_0, m_1"] & C \arrow[l, bend left] \end{tikzcd}$$

$k \overset{R}{\leftarrow} K$ unif. aleator aleasă

b $b \in \{0,1\}$

$c = Enc_k(m_b) = (c_{01}, c_{02})$
(c_{11}, c_{12})

CBC nu e CCA sigur

. Dacă

$m_0 = 0 \ldots 0$

$m_1 = 1 \ldots 1$

$c_0 = (iv, F_k(iv))$

$c_1 = (iv, F_k(iv \oplus (1 \ldots 1)))$

$c = (c_1, c_2)$

$c^1 = iv$

$c^2 = \begin{cases} F_k(iv) \\ F_k(iv) \oplus (1 \ldots 1) \end{cases}$

Daa 4

01.03.2016

$$\left.\begin{aligned} c' &= (iv, 0 \ldots 0) \\ m' &= iv \oplus F_k^{-1}(0 \ldots 0) \end{aligned}\right\}$$

— nu ne ajută

$c'' = (0 \ldots 0, c^2)$

$m'' = F_k^{-1}(c^2)$, $c^2 = \begin{cases} F_k(iv) \\ F_k(iv) \oplus (1 \ldots 1) \end{cases}$

indiferent de ramură, îl știm pe iv

Se întoarce $\begin{cases} iv \to c_0 \\ iv \oplus (1 \ldots 1) \to c_1 \end{cases}$

(5) ~~S-box~~

(8) AES.

$$\begin{bmatrix} 04 & 07 & E2 & 49 \\ F2 & 78 & 2F & C5 \\ CA & 28 & 01 & 17 \\ 97 & 45 & 96 & 10 \end{bmatrix}$$

$$\begin{bmatrix} 21 & 35 & AC & 6C \\ 75 & 50 & AF & 1B \\ 17 & 62 & 6B & F0 \\ 87 & 0B & 3C & 9B \end{bmatrix}$$ cheia de rundă

01.03.2016

1. ○ Sub bytes → pentru examen

într-un S-box

04
linie-col.
↓
F2

$$\begin{bmatrix} F2 & C5 & 98 & 3B \\ 89 & BC & 15 & A6 \\ 74 & 34 & 7C & 0E \\ 88 & 6E & 90 & CA \end{bmatrix}$$

2. ○ Shift rows

1 rând - identic
2 rând - rotește la stânga
:

$$\underbrace{\begin{bmatrix} F2 & C5 & 98 & 3B \\ BC & 15 & A6 & 89 \\ 7C & 0E & 74 & 34 \\ CA & 88 & 6E & CA \end{bmatrix}}_{S}$$

3. ○ Mix col

matrice standard

$$\underbrace{\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}}_{M}$$

$$(M \cdot S) \text{ MOD } F(x)$$

$$F(x) = x^8 + x^4 + x^3 + x + 1$$

Hexa	Binar		Polinom
		$x^3 x^2 x^1 x^0$	
01 =	0000	0001 =>	1
02 =	0000	0010 =>	x

$\boxed{34} \cdot \boxed{02}$

|| shiftare la stânga

$\boxed{0}$011 $\overset{.02.}{0100}$ => 0110 1000

↓
shiftare stânga ⊕ 0001 1011 → $\underbrace{\text{DOAR}}$, dacă primul bit e 1

(cele 4 operații) examen!

03 = 02 ⊕ 01

~~4.~~ Rezultat de la mix col:

$$\begin{bmatrix} 96 & 28 & C0 & 52 \\ 1F & 75 & 31 & FE \\ 73 & 4F & 64 & 71 \\ 42 & 44 & 31 & CB \end{bmatrix} = \text{Ieșire}$$

4. Add round key

Ieșire ⊕ cheia de rundă

96 ⊕ 21 => 1001 0110 ⊕ 0010 0001 =

= 1011 0111 => B7

12.04.2016

CRIPTO

- din seminarul 3

AES

$$\begin{bmatrix} 04 & 07 & E2 & 49 \\ 72 & 78 & 27 & C5 \\ CA & 28 & 01 & D7 \\ 97 & 45 & 96 & 10 \end{bmatrix}$$ intrarea

cheia $$\begin{bmatrix} 21 & 35 & AC & 6C \\ 75 & 50 & A7 & 1B \\ 17 & 62 & 6B & F0 \\ 87 & 0B & 3C & 9B \end{bmatrix}$$

0 4
linie coloană

ieșirea ?

1. Sub Byte

$$\begin{bmatrix} F2 & C5 & 98 & 3b \\ 89 & bC & 15 & a6 \\ 74 & 34 & 7c & 0e \\ 88 & 6e & 90 & ca \end{bmatrix}$$

2. Shift Rows

$$\begin{bmatrix} 72 & c5 & 98 & 3b \\ bc & 15 & a6 & 89 \\ 7c & 0e & 74 & 34 \\ ca & 88 & 6e & 90 \end{bmatrix}$$

3. Mix Columns

$$\left\{ \begin{array}{l} 01 = \overset{x^7}{0}000 \quad 00\overset{x^1}{0}\overset{x^0}{1} \Rightarrow 1 \quad \text{polinom} \\ 02 = 0000 \quad 0010 \Rightarrow x \end{array} \right.$$

$1\cancel{A} \cdot 02$

$\parallel$

$$\underset{x^4}{0001} \quad \overset{8421}{\underset{x^3 x^2 x^1 x^0}{1010}} = x^4 + x^3 + x \quad \Big| \cdot 02 = x \quad \Rightarrow$$

$$\Rightarrow x^5 + x^4 + x^2$$

$\parallel$

0011 0100

- 01 lasă pe loc
- 02 - dacă coef. lui $x^7 = 0$

  $\Rightarrow$ shiftare la stânga

  - dacă coef. lui $x^7 = 1$

  $\Rightarrow$ shiftare la stânga

  $\oplus$ 00011011

mod $f(x) = x^8 + x^4 + x^3 + x + 1$

$\Updownarrow$

$\oplus$ 0001 1011

shiftare :

$$\begin{array}{l} 0111\ 1000 \oplus \\ 0001\ 1011 \\ \hline 0110\ 0011 \oplus \\ 1011\ 1100 \\ \hline 1101\ 1111 \end{array}$$

.)

$$\begin{array}{l} 1111\ 1111 \oplus \\ 1101\ 1111 \\ 0111\ 1100 \\ 1100\ 1010 \\ \hline \underbrace{1001}_{9}\ \underbrace{0110}_{6} \end{array}$$

$$\Downarrow$$

96

$$\Rightarrow \begin{pmatrix} 96 & . & . & . \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \end{pmatrix}$$

4. Add Round Key

$96 \oplus 21$

$$\begin{array}{l} 1001\ 0110 \oplus \\ 0010\ 0001 \\ \hline 1011\ 0111 \end{array} \rightarrow \begin{bmatrix} B7 & . & . & . \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \end{bmatrix}$$

$\cdot 03 = 02 \oplus 01$

$nr \cdot 03 = nr \cdot 01 \oplus nr \cdot 02$

$$\begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix}$$

$F2 \cdot 02 \oplus \underbrace{C5 \cdot 01 \oplus 98 \cdot 01}_{\text{rămân la fel}} \oplus 3b \cdot \overset{03}{\cancel{02}} =$

·) $F2 \rightarrow 1111\ 0010$

$$\begin{array}{r} 11100100 \oplus \\ 00011011 \\ \hline 11111111 \end{array}$$

·) $3b \cdot 02$

$$\begin{array}{rr} 0011\ 1011 \rightarrow & 0111\ 0110 \oplus \\ & 0011\ 1011 \\ \hline & 0100\ 1101 \end{array}$$

·) ! Se calcula invers ↑ X

De fapt $03 \cdot bc$

$01 \cdot bc \oplus 02 \cdot bc$

$bc \rightarrow 1011\ 1100 \cdot 02$

(9) F PRF

$|m| = 2n - 2$

$m_0 \| m_1$ ($|m_0| = |m_1| = n-1$), $k \in \{0,1\}^n$

$t = F_k(0 \| m_0) \| F_k(1 \| m_1)$

Este CPA-sigur?

↳ nu trebuie să genereze un tag valid pentru alt mesaj în afara celor cerute deja

$$\begin{tikzcd} A \arrow[r, bend left, "m_0 \| m_1"] & \text{Oracol} \arrow[l, bend left, "F_k(0\|m_0) \| F_k(1\|m_1)"] \end{tikzcd}$$

Trimitem $m_0 \| m_0$ întoarce $F_k(0 \| m_0) \| F_k(1 \| m_0)$

Trimitem $m_1 \| m_1$. Întoarce $F_k(0 \| m_1) \| F_k(1 \| m_1)$

$m_0 \| m_1 \Rightarrow F_k(0 \| m_0) \| F_k(1 \| m_1)$

(7) 56 biți ← len

parola 8 caractere (64 biți)

↓

56

a) 2^{56}

spațiul cheilor

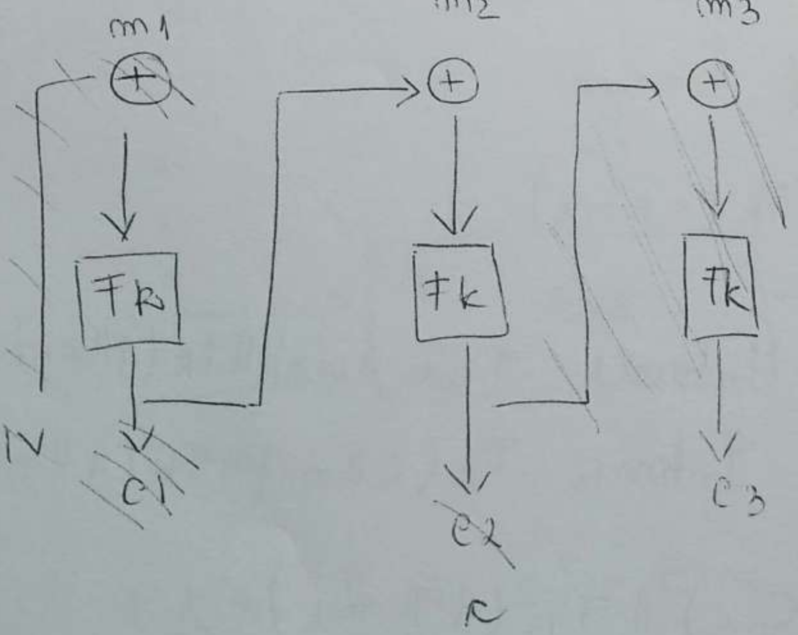
10^6 chei / secundă

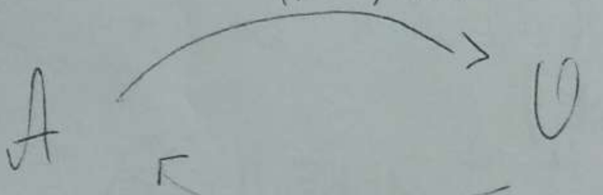
$\frac{2^{56}}{10^6}$ secunde

b) $(2^6)^8 = 2^{48} \rightarrow \frac{2^{48}}{10^6}$ secunde

c) $13^8 \rightarrow \frac{13^8}{10^6}$ secunde

(10) CBC MAC nu e sigur pt. mesaje de lung. dif.





$F_k(m), F_k(F_k(m_1) \oplus m_2)$

nu mai zic nimic

după

ne mănâncă la final

$m \to F_k(m)$

$0 \to F_k(0)$

$0 \parallel F_k(0) = F_k(F_k(0) \oplus F_k(0)) \to F_k(0)$

(11)

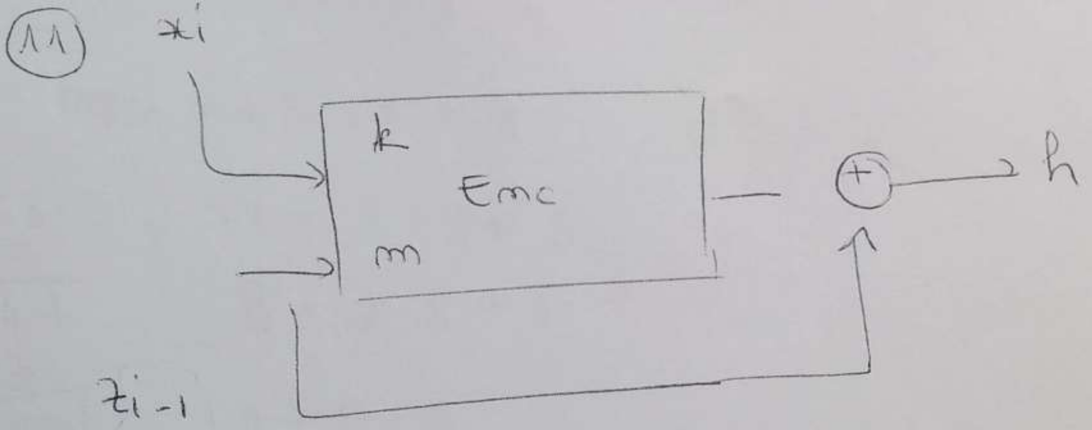
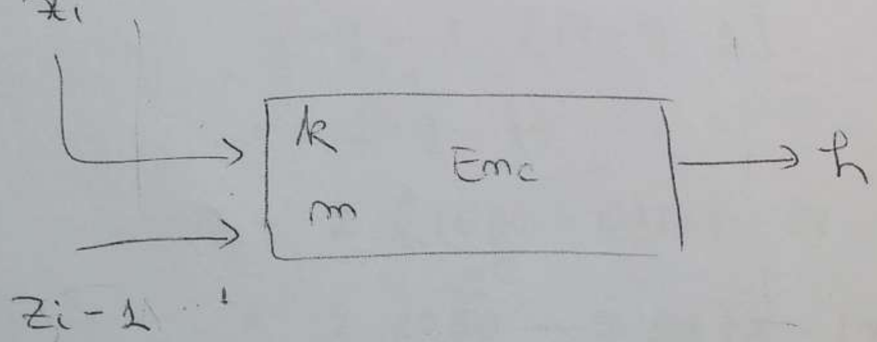


figura 1



(2

0

$h(x_i \parallel z_{i-1}) = Emc_{x_i}(z_{i-1})$

$h(x'_i \parallel z'_{i-1}) = Emc_{x'_i}('z_{i-1})$

$\boxed{x'_i} \parallel z'_{i-1} \neq x_i \parallel z_{i-1}$

$Emc_{x_i}(z_{i-1}) = Emc_{x'_i}(z'_{i-1})$

Fixăm x'_i, x_i, z_{i-1}

"Dobar dan!" = Bună ziua

$$z'_{i-1} = \mathrm{Dec}_{x'_i}\left(\underbrace{\mathrm{Enc}_{x_i}(z_{i-1})}_{\text{cunoaștem}}\right)$$ → deci se produce coliziune 5

26.04.2016

S5

CRIPTO

② $p=31$, $q=37$, $e=17$

$\phi(N) = (p-1)(q-1) = 30 \cdot 36 =$

$1080 = 63 \cdot 17 + 9$

```
 63·
 17
----
 441
 63
----
 1071
```

$17 = 1 \cdot 9 + 8$

$9 = 1 \cdot 8 + 1$

$1 = 9 - 8$

$= 9 - 8 \cdot 1$

$= 9 - 1 \cdot [17 - 9 \cdot 1]$

$= 2 \cdot 9 - 17$

$= 2(1080 - 63 \cdot 17) - 17$

$= \overbrace{2 \cdot 1080}^{=0} - 2 \cdot 63 \cdot 17 - 17$

mod 1080

$= -17(2 \cdot 63 + 1) = -17 \cdot 127$

$d = 17^{-1} = 1080 - 127 = 953$

③ Alice (pk_A, sk_A)

Bob (pk_B, sk_B)

a) $k \xleftarrow{R} K$

$$\begin{tikzcd} A \arrow[r, bend left, "\mathrm{Enc}(pk_B, k)"] & B \end{tikzcd}$$

(pk_A, sk_A) (pk_B, sk_B)

~~1.~~ Alice alege aleator o cheie și o trimite lui Bob. (criptarea cheii)

b)

$$\begin{tikzcd} \overset{k_1}{A} \arrow[r, bend left] & \overset{k_2}{B} \end{tikzcd}$$

(pk_A, sk_A) (pk_B, sk_B)

$Key = k_1 \oplus k_2$

↓ Alice trimite o cheie k_1 care e XOR-ată cu cheia k2 de la Bob.

④ (G, q, g) $\boxed{(G, \cdot)}$

A B

$x \in_R G$ $y \in_R G$

Cunoaștem: G, g, q (ordinul grupului)
↓ grup ↓ generator

$h_1 = g^x$ $h_2 = g^y$

$$\begin{tikzcd} A \arrow[r, bend left=0, shift left, leftarrow, "h_2"] \arrow[r, shift right, "h_1"'] & B \end{tikzcd}$$

$h = g^{xy} = (h_2)^x$ $h = g^{xy} = (h_1)^y$

$\boxed{(G, +)}$

(G, q, g)

A

$x \in_R G$

$h_1 = g \cdot x$

B

$y \in_R G$

$h_2 = g \cdot y$

$\xleftarrow{h_2}$

$\xrightarrow{h_1}$

$h = g \cdot x \cdot y = (h_2) \cdot x$

$h = g \cdot x \cdot y = h_1 \cdot y$

<u>NU</u> e sigur

$(h_1 \cdot h_2) : g$

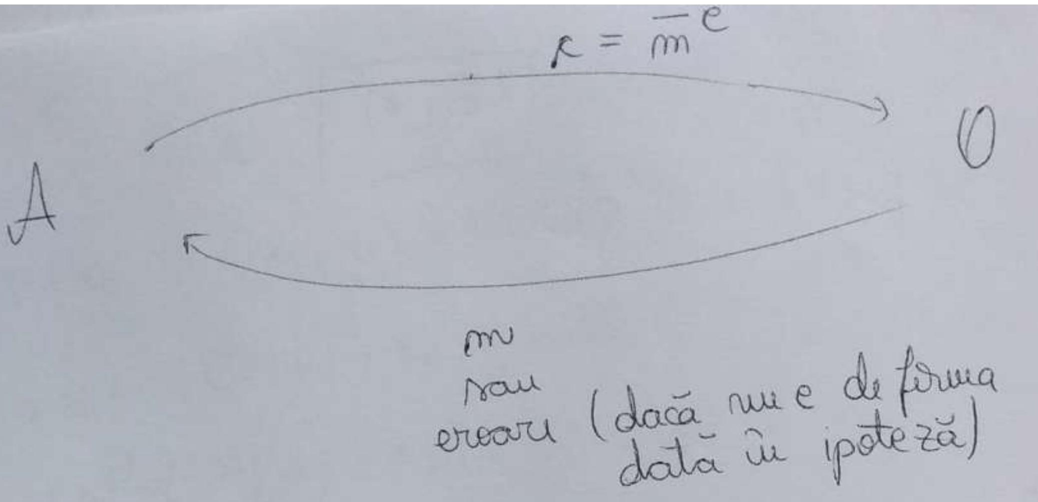
(5) $|m| = m \simeq |N| / 2$

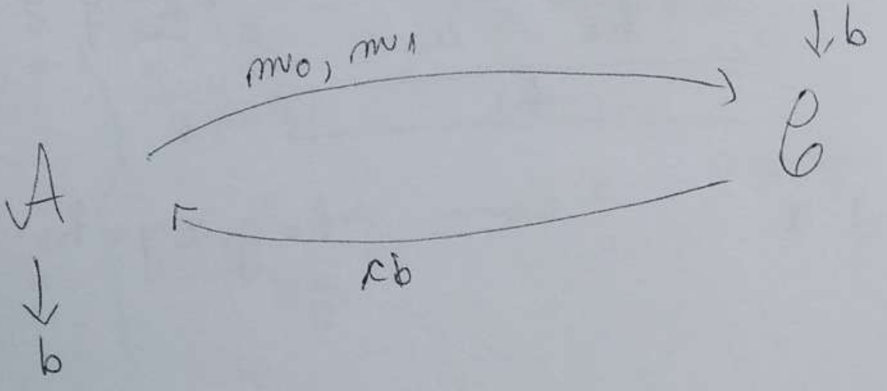
$\bar{m} = 0^k \| r \| 0^8 \| m$

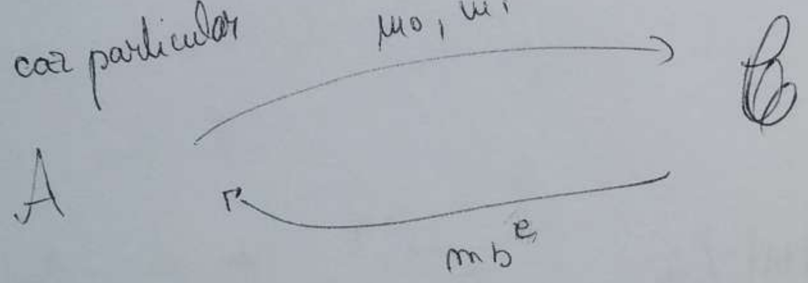
$r \xleftarrow[R]{} \{0,1\}^{80}$

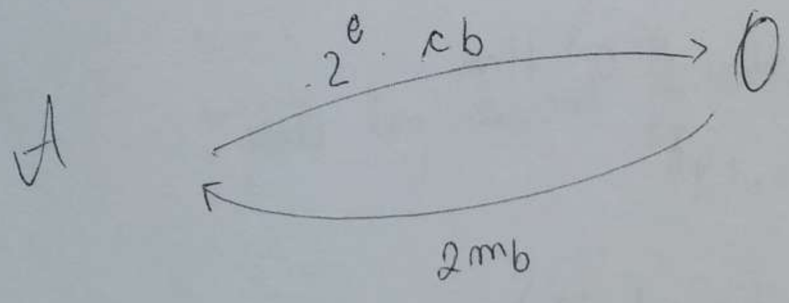
$c = \bar{m}^e \pmod N$

nu e CCA sigur









—

Trimitem mai multe perechi m_0, m_1 (m_0 cu 1 pe prima poziție, m_1 cu 0 pe prima poziție). Pt. m_0 primim eroare (pt. că nu se respectă formatul) (Shiftăm și vedem dacă întoarce eroare. Dacă întoarce eroare, fie a intrat peste 0^k fie peste 0^8).

nu intră
la examen
curbe eliptica

Prob. 7 $y^2 = x^3 + \underbrace{2}_{a}x + \underbrace{3}_{b} \mod \underbrace{17}_{p}$

$P + Q = (x_1, y_1) + (x_2, y_2) = (x_3; y_3)$

$x_3 = s^2 - x_1 - x_2 \mod p$

$y_3 = s(x_1 - x_3) - y_1 \mod p$

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \mod p, & P \neq Q \\ \dfrac{3x_1^2 + a}{2y_1} \mod p, & P = Q \end{cases}$$

$(G, \cdot) \rightarrow (E, +)$

$g \rightarrow P$

$x, g^x \rightarrow x ; \underbrace{P + \ldots + P}_{x}$

$P, xP ; \underbrace{x = ?}$ prob. log. discret pe curba eliptică