2.03.2016.

ALGEBRĂ
CURS 2

Alg. de criptare RSA. ≃ 1978. Rivest Shamir Adleman

<u>Teorema Euler</u> $\left.\begin{array}{l}(a,n)=1\\ a\in\mathbb{Z},\ n\in\mathbb{N}^*\end{array}\right\} \Rightarrow a^{\varphi(n)}\equiv 1 \pmod{n}$

$\varphi(n)=|U(\mathbb{Z}_n)| = n\cdot\prod_{\substack{p \text{ prim} \\ p|n}}\left(1-\frac{1}{p}\right)$

<u>Consecința</u>: n prim

$\left.\begin{array}{l}\varphi(n)=n-1\\ n \nmid a\end{array}\right\} \Rightarrow a^{n-1}\equiv 1\pmod{n}$

Mica Th. a lui Fermat.

(n, e) $\quad (e, \varphi(n))=1$

$n = p\cdot q$ $\quad \varphi(n)=\varphi(pq)=pq\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)$

$p<q$ $\quad =(p-1)(q-1)$

p, q - prime

Alfabet: de lungime 26 - pt. început.

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
0	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

mesaj → nr.

$26^k < n < 26^{k+1}$.

Se împarte textul în secv. de lung k

O secv. de lung k se va transforma în una de lung k+1.

$a_{k-1} a_{k-2} a_{k-3} \ldots a_0 \longrightarrow a_0 + 26 a_1 + 26^2 a_2 + \ldots + 26^{k-1} a_{k-1} = P$

$P^e \pmod n$

↳ il scriu în baza 26 = $b_k b_{k-1} \ldots b_0{}_{(26}$

exemple:

$\begin{cases} n = ~~209~~\ 851. \\ e = 53 \end{cases}$ NU $\longrightarrow$

$26^k < ~~209~~\ 851 < 26^{k+1}$

$26 < 209 < 26^2 = 676.$

$k = 1.$

└─┘ ⟶ └─┘└─┘ — o lit se va transf în 2.

N=13.

ex: $\begin{cases} n = 851. \\ e = 109 \end{cases}$ NU $\longrightarrow$

$26^2 < 851 < 26^3$

└┘└┘ ⟶ └┘└┘└┘ 2 lit în 3.

NU $\longrightarrow 13 \cdot 26 + 20 = 338 + 20 = 358$

(N = 13, U = 20)

$358^{109} \equiv_{851}$

Fol. l. chin a rest:

$851 = 37 \cdot 23$

$$358^{109} \overset{37}{\equiv} 25^{109} = (25^{36})^3 \cdot 25 \overset{37}{\equiv} 25$$

$$\begin{array}{r|l} 358 & 37 \\ 333 & 9 \\ \hline =25 & \end{array}$$

acum fol mica th. Fermat

$$25^{36} \equiv 1 (37)$$

$$358^{109} \overset{23}{\equiv} 13^{109} \overset{23}{\equiv} -7 \overset{23}{\equiv} 16.$$

$$13^{22} \equiv 1 (23)$$

$$13^{110} \equiv 1 (23)$$

$$13x \equiv 1 (23) \mid \cdot 2$$

$$13x \equiv 26x \equiv 2 (23) \equiv -21 \Rightarrow x \equiv \frac{-21}{3} = -7.$$

$$x \equiv -7$$

$$A = 37t + 25 \overset{23}{\equiv} 16$$

$$14t \overset{23}{\equiv} 16 - 25 = -9 \overset{23}{\equiv} 14 \qquad t \equiv 1$$

$$A = 37(23s+1) + 25 = 851s + 37 + 25 = 851s + 62.$$

$$358^{109} \overset{851}{\equiv} \boxed{62}$$

$$62 = 26^2 \cdot 0 + 26 \cdot 2 + 10$$

NU → ACK.

0, 2, 10

↓ ↓ ↓

A C K

Decryption

1) Gasim p, q $\quad (e, \varphi(n)) = 1.$

2) Rezolvam $e \cdot f \equiv 1 \pmod{\varphi(n)}$

$p = 37.$
$q = 23.$

$\varphi(n) = n - p - q + 1$

$= pq - p + q + 1 = (p-1)(q-1)$

3) Q^f

$109 f \equiv 1 (792) \mid \cdot 7.$

$-29 \equiv 763 f \equiv 7 (792)$

$792 = 22 \cdot 36.$

$792 - 763 = 29.$

$f = 109.$

$62^{109} \overset{851}{\equiv}$

AB $\longrightarrow$ C D E

I $26 \cdot A + B$ $\qquad$ $C \cdot 26^2 + D \cdot 26 + E$

Rivest, Shamir, Adleman.

inele de polinoame R. inel comutativ.

Def: Un inel $(R,+,\cdot)$ s.n. comutativ dacă $a\cdot b = b\cdot a$. $\forall a,b \in R$.

$f: \mathbb{N} \to R$.
$f(n) = 0 \quad \forall n \geq n_0 + 1$

↳ polinom
$f(0) + f(1)X + f(2)X^2 + \dots + f(n_0)X^{n_0}$

$f = g \overset{def}{\iff} f(n) = g(n) \quad \forall n \in \mathbb{N}$

f, g polinoame
$(f+g)(n) = f(n) + g(n) \quad \forall n \in \mathbb{N}$

$f \cdot g(n) = \sum_{k=0}^{n} f(k) \cdot g(n-k)$

$(R[X], +, \cdot)$ inel comutativ

$\operatorname{grad} f = \begin{cases} \max\{k \mid f(k) \neq 0\} & f \neq (0,0,0,\dots) \\ -\infty, & f = 0 \end{cases}$

$\operatorname{grad} f \cdot g \leq \operatorname{grad} f + \operatorname{grad} g$

$f(x) = a_k X^k + \dots + a_0$
$g(x) = b_n X^n + \dots + b_0$
$f \cdot g(x) = a_k \cdot b_n X^{n+k} + \dots$

$\begin{cases} a_k \neq 0 \\ b_m \neq 0. \end{cases}$

$\hookrightarrow a_k \cdot b_m \neq 0.$

Dacă R corp $\Rightarrow \text{grad}\, f \cdot g = \text{grad}\, f + \text{grad}\, g$

Def: $(R, +, \cdot)$ inel.
R s.m. corp dacă $U(R) = R \setminus \{0\}$

R corp $x \neq 0, y \neq 0 \Rightarrow x \cdot y \neq 0$ R inel comutativ.

Presupun că: $x \cdot y = 0$.

$x \neq 0 \Rightarrow \exists\, r \in R$ a.î. $r \cdot x = x \cdot r = 1$.

$y = 1 \cdot y = (r \cdot x) \cdot y = r(xy) = r \cdot 0 = 0$. ↯

Rădăcină a unui polinom

$f(x) = a_k x^k + \ldots + a_1 x + a_0$

Unui polinom îi asociem o funcție polinomială.

$f(x) = a_k \cdot x^k + \ldots + a_1 x + a_0$

$x \in R$ s.m. rad a lui f dacă $f(x) = 0$.

Proble: nr. rad ale lui f este cel mult gradul lui f.

$f(x) = x^3 - x \in \mathbb{Z}_6[x]$

$f(\bar{0}) = \bar{0}$
$f(\bar{1}) = 0.$
$f(\bar{2}) = \bar{8} - \bar{2} = \bar{6} = \bar{0}$
$f(\bar{3}) = \overline{27} - \bar{3} = \overline{24} = \bar{0}$
$f(\bar{4}) = 60 = \bar{0}$
$f(\bar{5}) = \overline{120} = \bar{0}$

$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$.

↙ corpul cuaternionilor.

$a + bi + cj + dk = a_1 + b_1 i + c_1 j + d_1 k$.

$\Leftrightarrow \begin{cases} a = a_1 \\ b = b_1 \\ c = c_1 \\ d = d_1 \end{cases}$.

$(a + bi + cj + dk) + (a_1 + b_1 i + c_1 j + d_1 k) =$

$= a + a_1 + (b + b_1) i + (c + c_1) j + (d + d_1) k$.

$\boxed{i^2 = j^2 = k^2 = -1}$

$i \cdot j = k$ $\quad j \cdot k = i$, $k \cdot i = j$.

$j \cdot i = -k$ $\quad k \cdot j = -i$ $\quad i \cdot k = -j$

$(\mathbb{H}, +, \cdot)$ - corp necomutativ.

$f(x) = x^2 + 1$.

↳ f are o infinitate de rădăcini în $\mathbb{H}$

K - corp. comutativ. $\quad f \in K[X], f \neq 0 \Rightarrow \exists\, K$ corp comut. $K \subseteq K_1$.

a.î. f are grad f rădăcini în K

$(\mathbb{C}, +, \cdot)$, $f \in \mathbb{C}[X]$, $f \neq 0 \Rightarrow f$ are toate rad în $\mathbb{C}$