Criptografie - Tema 3

Nr 2

3) $2^n - 1$ prim $\Rightarrow$ n prim

Pt $n \leq 3$ obținem concluzia prin verificare

$n = 0 \Rightarrow 2^0 - 1 = 0$ (nu e prim)

$n = 1 \Rightarrow 2^1 - 1 = 1$ (nu e prim)

$n = 2 \Rightarrow 2^2 - 1 = 3$ (e prim și $n = 2$ e prim)

$n = 3 \Rightarrow 2^3 - 1 = 7$ (e prim și $n = 3$ e prim)

Pp $n > 3$

Pp prin R.A. că n nu e prim $\Rightarrow$

$\Rightarrow \exists k, t \in \mathbb{N}^* \setminus \{1\}$ a.î. $n = k \cdot t$

$$2^n - 1 = 2^{k \cdot t} - 1 = (2^k)^t - 1 =$$

$$= \underbrace{(2^k - 1)}_{\in \mathbb{N}} \underbrace{\left((2^k)^{t-1} + (2^k)^{t-2} + \ldots + (2^k)^1 + 1\right)}_{\in \mathbb{N}}$$

$k \in \mathbb{N}^* \setminus \{1\} \Rightarrow 2^k - 1 > 1$

$2^k < 2^n \Rightarrow 2^k - 1 < 2^n - 1$

$\Rightarrow 2^n - 1$ are un divizor diferit de 1 și de el însuși $\Rightarrow$

$\Rightarrow 2^n - 1$ nu e prim (contradicție cu ip)

9)2) $n = 21803$

$n - 1 = 21802$

$21802 \mid 2$
$10901 \mid = 10901$
1

$n - 1 = 2 \cdot 10901$

$b^{n-1} = (b^{10901})^2$

(*) $(b^{10901})^{2^{\wedge}} \equiv 1 \pmod{n}$

Deci nu aparem le 1 sau înainte de 1 nu

avem -1 $\Rightarrow$ n compus

Mulțor $b = 2$

$(2^{10901})^{2^0} = 2 \cdot (2^2)^{5450} = 2 \cdot (4^2)^{2725} =$

$= 32 \cdot (16^2)^{1362} = 32 \cdot (256^2)^{681} =$

$= 32 \cdot 127 \cdot (127^2)^{340} = 4064 \cdot (16129^2)^{170} =$

$127 \cdot$
127
889
254
127
16129

$256 \cdot$
256
1536
1280
512
65536

$65536 : 21803 = 3$
65409
127

$= 4064 \cdot (13048^2)^{85} =$

$= 4064 \cdot 12480 \cdot (12480^2)^{42}$

~~[illegible]~~ .

$= 4942 \cdot (11571^2)^{21} =$

$= 4942 \cdot 17621 \cdot (17621^2)^{10} =$

$16129 \cdot 16129 = 260144641$

$260144641 : 21803 = 11931$

21803

$= 42114$

21803

203116

196227

6889

6409

$= 3489$

21803

13048

$= 1800 \cdot (3118^2)^5 = 1800 \cdot 19589 \cdot (19581^2)^2 =$

$= 4749 \cdot 2571 \equiv 21802 \pmod{21803}$

$(2^{10901})^2 = 21802^2 \equiv 1 \pmod{21803} \Rightarrow$

$\Rightarrow$ n poate fi prim

Martor $b = 3$

$3^{10901} = 3 \cdot (3^2)^{5450} = 3 \cdot (9^2)^{2725} = 3 \cdot 81 \cdot (81^2)^{1362} =$

$= 243 \cdot (6561^2)^{681} = 243 \cdot 7599 \cdot (7599^2)^{340} =$

$= 15105 \cdot (10457^2)^{170} = 15105 \cdot (6805^2)^{85} =$

$= 15105 \cdot 6657 \cdot (6657^2)^{42}$

$= 120 \cdot (9731^2)^{21}$

$= 120 \cdot 1932 \cdot (1932^2)^{10}$

$= 13810 \cdot (4311^2)^5 =$

$= 13810 \cdot 8565 \cdot (8565^2)^2$

$= 1375 \cdot 16380 \equiv 1 \pmod{n}) \Rightarrow$

$\Rightarrow n$ ~~e compus~~

NU e prim, n e compus