RC
(L12)

19.05.2021

Diffie Hellman

→ Fie p – număr prim
α – $\underbrace{\text{rădăcina primitivă}}$ a lui p

$\alpha^1 \% p, \alpha^2 \% p, \dots, \alpha^{(p-1)} \% p$ au rezultatele $1, 2, 3, \dots, p-1$, dar nu neapărat în această ordine (și să nu se repete)

→ Exemplu:
Considerăm $p = 7$ și $\alpha = 3$.

$$\left.\begin{array}{l} 3^1 \% 7 = 3 \\ 3^2 \% 7 = 2 \\ 3^3 \% 7 = 6 \\ 3^4 \% 7 = 4 \\ 3^5 \% 7 = 5 \\ 3^6 \% 7 = 1 \end{array}\right\}$$

nu se repetă și avem tot intervalul =) =) „α" este rădăcina primitivă a lui „p"

→ Fie calculatoarele A și B
- A și B aleg câte un număr aleator mai mic ca „p"
- notăm X_A și X_B numerele alese de gazdele A și B.
- se calculează numerele Y_A și Y_B astfel:

$$Y\_A = \alpha^{(X\_A)} \% p$$

$$Y\_B = \alpha^{(Y\_B)} \% p$$

- A îi trimite lui B valoarea Y_A.
- B îi trimite lui A valoarea Y_B.
- A calculează cheia de criptare:

$$K = (Y\_B)^{(X\_A)} \% p$$

- B calculează cheia de criptare:

$$K = (Y\_A)^{(X\_B)} \% p$$

e aceeași

→ Exemplu:

$p = 7$; $\alpha = 3$; $X\_A = 1$; $X\_B = 2$

$Y\_A = 3^1 \% 7 = 3$

$Y\_B = 3^2 \% 7 = 2$

A și B schimbă între ele valorile lui Y_A și Y_B

A: $K = 2^1 \% 7 = 2$

B: $K = 3^2 \% 7 = 2$