Diffie Hellman ≃ 1975 (DHE)

Dacă p ∈ ℙ

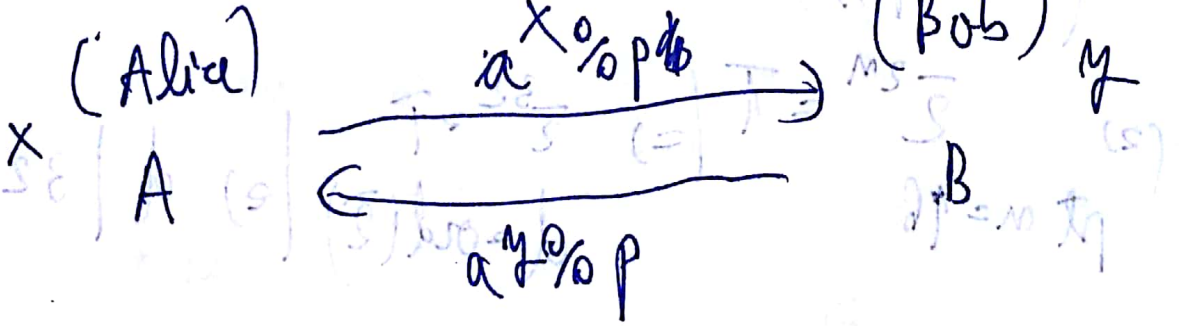
$(U(2p), \cdot)$ – grup ciclic

$U(2p) = \{\bar{1}, \bar{a}, \bar{a}^2, \ldots, \bar{a}^{p-1}\}$

$|U(2p)| = \varphi(p) = p-1$

ord $\bar{a}$ este în G $\Rightarrow (\text{ord}\,\bar{a}) \mid p-1 \Rightarrow \text{ord}\,\bar{a} = p$.

// definiția ordinului



(p, q) publi

(oneal)

1/

cheia comună a^{xy}

Numere prime mari $\begin{cases} 2^q+1 \\ (2^q-1) \end{cases}$

Ex: 2^m+1 prim atunci $m=2^n$

Dem că $2^{16}+1$ prim

Fie p prim $p \mid (2^m+1)$ $d = ord(\bar{2})$ $\Rightarrow d \mid (p-1)$

$\overline{2^m+1} = \bar{0} \Leftrightarrow \overline{2^m} = -\bar{1} \Rightarrow$

$\Leftrightarrow \bar{2}^{2m} = \bar{1} \Leftrightarrow \bar{2}^{32} = \bar{1}$

pt $n=16$

$d = ord(\bar{2}) \mid 32 \Rightarrow$

$d \in D_{32}$

$ord\,\bar{2} \neq 16 \Rightarrow \ldots \Rightarrow d = ord\,\bar{2} = 32 \Rightarrow$

$ord\ \bar{2}^{16} = -1$

$\Rightarrow 32 \mid (p-1) \Rightarrow p \geq 1+32t$

2/

$t=1 \Rightarrow p=33$ ✗

$t=2 \Rightarrow p=65$ ✗

$t=3 \Rightarrow p=97$ ✓

$t=4 \Rightarrow p=129$ ✗

$t=5 \Rightarrow p=161 : 7$ ✗

$t=6 \Rightarrow \boxed{p=193}$

$2^{2^n}+1$ - prim pentru $n \in \{0,1,2,3,4\}$

Categoria 2^n-1

$2^{74207281}-1$ - (exponentul zilei)

EX: dacă 2^n-1 - prim $\Rightarrow$ n prim

Cele mai mari nr prime explicite

n par

- nr perfect par $n = 2^{n-1}(2^n-1)$

Dem: 2^{n-1} prim (cel mai mare în antichitate)

$2^{13}-1$ 2 8 1 9 1

$\sqrt{8191} = 90,\ldots$

$\hat{2}^{13} = \hat{1}$, $\operatorname{ord} \hat{2} = 13$

$13 \mid (p-1) \Leftrightarrow p = 1 + 13t$

$t = 2, 4, 6$

$\Rightarrow p = 27$

$\Rightarrow p = 53$

$\Rightarrow p = 79$

~~3) p~~

$2^{13} - 1$ nr prim

la fel repede demonstra și pentru $2^{11} - 1$

4) $\operatorname{ord} g^K = \dfrac{\operatorname{ord} g}{\gcd(K, \operatorname{ord} g)}$

5) $(G, \cdot)$ grup comutativ

$\gcd(\operatorname{ord} a, \operatorname{ord} b) = 1 \Rightarrow \operatorname{ord}(a \cdot b) = \operatorname{ord} a \cdot \operatorname{ord} b$

$a, b \in G$

// de demonstrat la seminar 4 și 5

4/.

Grupuri de permutări

$n \in \mathbb{N}^*$

$S_n = \{ f : \{1, 2, \dots, n\} \to \{1, 2, 3, \dots, n\} \mid f \text{ bij} \}$

$(S_n, \circ)$ - grup

$f, g \in S_n$

$f \circ g : \{1, 2, 3, \dots n\} \to \{1, 2, \dots, n\}$

$(f \circ g)(j) = f(g(j)), \forall j = \overline{1, n}$

Ex: grup necomutativ. De ce? găsim 2 elemente care nu comută

Obs $|S_n| = n!$

Signatura unei permutări

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(i) - \sigma(j)}{j - i} \in \{\pm 1\}$$

// Definiția inversiunii

(i, j) - inversiune $i < j$

$\sigma(i) > \sigma(j)$

Prop:
$\varepsilon(\sigma \circ \tau) = \varepsilon(\sigma) \cdot \varepsilon(\tau)$
– vezi de demonstrat folosind formula

Ordinul unei permutări

$k \in \mathbb{N}^*$ minim ai $\sigma^k = e$ – permutarea identică

Ciclul unei permutări

$(a_1, a_2, \dots, a_k)$ $\quad a_1, a_2, \dots, a_k \in \{1, 2, \dots, n\}$, $a_i \neq a_j \ \forall i \neq j$, $1 \leq i, j \leq k$

$$\begin{cases} \sigma(a_k) = a_1 \\ \sigma(a_j) = a_{j+1} \end{cases} \quad 1 \leq j < k$$

Notăm ciclul cu o permutare σ

Spunem că
$(a_1, a_2, \dots, a_n)$ și $(b_1, b_2, \dots, b_m)$ sunt disjuncte
dacă $\{a_1, a_2, \dots, a_n\} \cap \{b_1, b_2, \dots, b_m\} = \emptyset$

dacă sunt, atunci ele două cicli comută

ord (ciclu) = k

E/

$\tau = (a_1, a_2, \dots, a_k)$

~~$\tau^2 = ($~~

$\tau^k(a_1) = \tau^{k-1}(\tau(a_1)) = \tau^{k-1}(a_2) = \dots$

$= \dots = a_1$ - inductiv

cu k este cel mai mic nr cu această proprietate

2 cicli disjuncți

$\text{ord}((a_1, a_2, \dots, a_k)(b_1, b_2, \dots, b_t)) = [k, t]$

cel mai mic multiplu comun

$\sigma = (a_1, a_2, \dots, a_k) \circ (b_1, b_2, \dots, b_t) \circ \dots \circ$ ~~σ^k~~

~~$= \sigma^k$~~ cicli disjuncți

$\text{ord}\,\sigma = [k, t, \dots]$

Împărțirea cifrelor

Problemă bonus

$A, B, C, D, \dots$ Σ

$\sigma \in S_{26}$

scriem un text cu o permutare

$-\{K, Q, X, Y, W\}$

BM HA BLPIOCB PHZOARODIZB PHOM

NMBPGHANOHI MAZOPDELO MOP SEF

MIHEMN MOPDIZARVO RBPOHI