Przypomnienie

$\mathbb{Z}_p^* = (\{1, 2, \ldots, p-1\}, \cdot)$ – grupa cykliczna. $p \in \mathbb{P}$.

Protokół Diffie – Hellmana.

Problemy obliczeniowe w grupie $\mathbb{Z}_p^*$:

1. Potęgowanie, Niech $g \in \mathbb{Z}_p^*$, $n \in \mathbb{N}$

Złożoność obliczeniowa g^n to około $\log_2 n$.

np: $g^{48} = g^{32} \cdot g^{16}$ $(g^2)^{2222} \cdot (g^2)^{222}$.

Potęgowanie jest łatwe.

2. Problem Logarytmu dyskretnego
Niech $g \in \mathbb{Z}_p^*$ – generator, $a \in \mathbb{Z}_p^*$
Podaj $n \in \mathbb{N}^+$ takie że $g^n = a$.

Złożoność to około n.

3. Niech $g \in \mathbb{Z}_p^*$ generator, $a, b \in \mathbb{Z}_p^*$
wtedy istnieją $m, n \in \mathbb{N}$ $g^m = a$, $g^n = b$.
Oblicz $c = g^{m \cdot n}$.

- Cel protokołu, aby osoby A i B komunikując się otwartym kanałem i nie mając ustalonego wcześniej wspólnego sekretu ustaliły sekret znany tylko A i B.

Protokół.

0. Ustalamy $p \in \mathbb{P}$ tak aby problem obliczeniowy 3 był trudny a 1 łatwy. Wybieramy $g \in \mathbb{Z}_p^*$ generator.

! p i g są jawne!

A		B
1. A wybiera losowo $n \in \mathbb{N}^+$		
Wylicza $a = g^n$		
Przesyła a do B	$\xrightarrow{a}$	2. Wybiera $m \in \mathbb{N}^+$
		Oblicza $b = g^m$
	$\xleftarrow{b}$	Przesyła b do A
3 A oblicza		4. B oblicza
$S_A = b^n$		$S_B = a^m$

Wtedy $S_A = b^n = (g^m)^n = g^{m \cdot n} = g^{n \cdot m} = (g^n)^m = a^m = S_B$

jest wspólnym sekretem A i B.

Bezpieczeństwo:

Załóżmy że istnieje sposób na złamanie protokołu: tzn Osoba podsłuchująca kanał komunikacji potrafi odgadnąć sekret $S_A = S_B$.

Osoba podsłuchująca zna $p \in \mathbb{P}$, $g \in \mathbb{Z}_p$, $a = g^n$, $b = g^m$.

i potrafi obliczyć $S_A = g^{m \cdot n}$.

To znaczy podsłuchujący rozwiązuje problem 3.

- Chińskie twierdzenie o resztach.

$k \in \mathbb{Z}$.
$k, n \in \mathbb{N}$ to $k \pmod n$ oznacza resztę z dzielenia k przez n

Uwaga. Niech $m, n \in \mathbb{N}$ to wtedy
$\forall k \in \mathbb{Z} \quad (k \pmod n) \pmod m = k \pmod m$.

Np $k \pmod{10} \bmod 5 = k \pmod 5$

Fakt Jeśli $m \mid n$ to funkcja
$\varphi_m(k) = k \pmod m : C_n \to C_m$
jest homomorfizmem grup.

Dowód $\varphi_m(k +_n l) = \underbrace{(k +_n l) \bmod m} = \underbrace{(k+l) \bmod n} \pmod m$

$\overset{n}{=} (k+l) \pmod m = k \pmod m +_m l \bmod m =$
$\varphi_m(k) +_m \varphi_m(l)$ □

TW Niech $p, q \in \mathbb{N}$, $NWD(p,q) = 1$. Wtedy funkcja

$\varphi(k) = (k \bmod p, k \bmod q) : C_{p \cdot q} \to C_p \times C_q$
jest izomorfizmem grup.

Dowód. Skoro $p \mid p \cdot q$ to $\varphi_p(k) = k \bmod p$ jest homomorf
$\varphi_p : C_{pq} \to C_p$

$q \mid pq$ to $\varphi_q = k \bmod q : C_{pq} \to C_q$
jest homomorf.

?!! Wiec : $\varphi(k) = (\varphi_p(k), \varphi_q(k)) : C_{pq} \to C_p \times C_q$
jest homomorf.

φ jest na: $|\mathrm{Im}\,\varphi| = p \cdot q$

Pokazaliśmy że w $\mathrm{Im}\,\varphi$ istnieje element rzędu $p \cdot q$:

$$\mathrm{ord}(\varphi(1)) = \mathrm{ord}(1,1) = \mathrm{NWW}(\mathrm{ord}_{C_p}(1), \mathrm{ord}_{C_q}(1)) = \mathrm{NWW}(p,q) = p \cdot q$$

Wiemy: $\langle \varphi(1) \rangle \leq \mathrm{Im}(\varphi)$

$pq = |\langle \varphi(1) \rangle| \leq |\mathrm{Im}(\varphi)| \leq pq$

Zatem $|\mathrm{Im}\,\varphi| = p \cdot q$, więc $\mathrm{Im}\,\varphi = C_p \times C_q$, więc φ jest na.

Więc φ jest bijekcją. (zbiory są skończone).

Zatem φ jest izomorfizmem. □

Wniosek(*) Jeśli $q_1, q_2 \dots q_n$ parami względnie pierwsze to funkcja

$$\varphi(k) = (k \pmod{q_1}, k \pmod{q_2}, \dots, k \pmod{q_n})$$

$$\varphi : C_{q_1 q_2 \dots q_n} \longrightarrow C_{q_1} \times C_{q_2} \times \dots \times C_{q_n}$$

jest izomorfizmem.

D-d dla 3. $q_1\ q_2\ q_3$ parami wzg pierwsze

$$C_{q_1 q_2 q_3} \longrightarrow C_{q_1} \times C_{q_2 q_3}$$

$$\varphi'(k) = (k \bmod q_1, k \bmod q_2 q_3)$$

$$C_{q_1 q_2 q_3} \xrightarrow{\varphi'} C_{q_1} \times C_{q_2 q_3} \xrightarrow{\varphi''} C_{q_1} \times C_{q_2} \times C_{q_3}$$

$$k \xrightarrow{\varphi'} (k \bmod q_1, k \bmod q_2 q_3) \xrightarrow{\varphi''} (k \bmod q_1, k \bmod q_2, k \bmod q_3)$$

TW Chińskie twierdzenie o resztach.

Niech $q_1, q_2 \dots, q_n$ parami względnie pierwsze liczby $\mathbb{N}$ oraz $a_1, a_2 \dots, a_n \in \mathbb{Z}$. Wtedy istnieje $r \in \mathbb{N}$ takie, że:

$$\begin{cases} r \equiv a_1 \pmod{q_1} \\ r \equiv a_2 \pmod{q_2} \\ \vdots \\ r \equiv a_n \pmod{q_n} \end{cases}$$

Przykład $q_1 = 3$, $q_2 = 5$, $a = 2$, $b = 4$

TW: $\exists r$:

$$\begin{cases} r \equiv 2 \mod 3 \\ r \equiv 4 \mod 5 \end{cases}$$

$r = 14$

Założenie q_i są względnie pierwsze jest istotne:

Nie istnieje r: $\begin{cases} r \equiv 0 \mod 4 \\ r \equiv 1 \mod 2 \end{cases}$

Dowód twierdzenia.

Niech $q_1 \dots q_n$, $a_1 \dots a_n$ jak w założeniach twierdzenia.

bzo $a_i \in \{0, \dots q_i - 1\}$

Z wniosku (*) funkcja

$$\varphi(k) = (k \bmod q_1, \dots, k \bmod q_n) : C_{q_1 \cdot q_n} \longrightarrow C_{q_1} \times \dots \times C_{q_n}$$

jest izomorfizm. i więc jest na.

Więc istnieje $r \in C_{q_1 \dots q_n}$ takie że

$$\varphi(r) = (a_1, a_2 \dots, a_n)$$

Wtedy: $\varphi(r) = (r \bmod q_1, r \bmod q_2, \dots, r \bmod q_n) = (a_1, a_2 \dots a_n)$

Zeke $\begin{cases} r \bmod q_1 = a_1 \\ r \bmod q_2 = a_2 \\ \vdots \\ r \bmod q_n = a_n \end{cases}$ □

Przykład $R \begin{cases} r \equiv 1 \bmod 5 \\ r \equiv 3 \bmod 7 \end{cases}$

Mamy: $R \begin{array}{ll} r = 5k+1 & k \in \mathbb{Z} \\ r = 7l+3 & l \in \mathbb{Z} \end{array}$

Zeke

$R: \begin{array}{l} 5k+1 = 7l+3 \\ 5k-7l = 2 \end{array}$ $\quad k = l = -1$

Ogólne: rozwiązujemy algorytmem Euklidesa $\quad r = 5\cdot(-1)+1 = -4$

Pozostałe rozwiązania

Zauważmy że jeśli k, l oraz k', l' różne rozwiązania (R)

$$\begin{array}{l} r_1 = 5k+1 = 7l+3 \\ r_2 = 5k'+1 = 7l'+3 \\ \hline \end{array}$$

$$r_1 - r_2 = 5(k-k') = 7(l-l')$$

$$\left.\begin{array}{l} 5 \mid r_1 - r_2 \\ 7 \mid r_1 - r_2 \end{array}\right\} \longrightarrow 35 = 7\cdot 5 \mid r_1 - r_2$$

Pozostałe rozwiązania $(-4) + 35\cdot k \qquad k \in \mathbb{Z}$.