

Spis treści

1	Szyfr Shannona	1
1.1	Szyfr XOR	1
1.2	Bezpieczeństwo doskonałe	1
2	Struktury algebraiczne	1
2.1	Podgrupa	2
2.2	Generatory	2
2.3	Problem logarytmu dyskretnego	2
2.4	Warstwy	2
3	RSA	2
3.1	Definicja	3
3.2	Trudność problemu	3
3.3	Przykład	3

1 Szyfr Shannona

Szyfr według Shannon’a jest zdefiniowany jako:

$$\pi = (E, D) : (C, M, K)$$

gdzie schemat szyfrujący E i schemat deszyfrowania D są funkcjami:

$$E : M \times K \rightarrow C$$

$$D : C \times K \rightarrow M$$

$$D(k, E(k, m)) = m$$

1.1 Szyfr XOR

$$K = M = C = \{0, 1\}^L$$

$$E(m, k) = m \oplus k$$

$$D(c, k) = c \oplus k$$

1.2 Bezpieczeństwo doskonałe

Niech π będzie szyfrem Shannona. Rozważmy eksperyment losowy, w którym zmienna losowa K ma rozkład jednostajny nad K . Jeśli zachodzi:

$$\forall_{m_0, m_1 \in M} \forall_{c \in C} P(E(k, m_0) = c) = P(E(k, m_1) = c)$$

to mówimy, że szyfr π jest szyfrem doskonałym.

Jeśli π jest szyfrem doskonałym, to $|K| \geq |M|$.

2 Struktury algebraiczne

1. $\forall_{a, b \in G} a * (b * c) = (a * b) * c$
2. $\forall_{a, b \in G} a * b = b * a$
3. $\exists_{e \in G} \forall_{a \in G} a * e = a$
4. $\forall_{a \in G} a^{-1} = e$

- półgrupa: 1
- monoid: 1, 3
- grupa: 1, 3, 4
- grupa abelowa: 1, 2, 3, 4

Zawsze istnieje tylko jeden element neutralny operacji. Rzędem grupy jest moc zbioru G .

$$\varphi(n) = |\{a \in \mathbb{Z}_n : \gcd(a, n) = 1\}|$$

2.1 Podgrupa

Niech H będzie podgrupą grupy G . Wtedy:

$$\forall a, b \in H \quad a * b \in H$$

$$\forall a \in H \quad a^{-1} \in H$$

Na przykład, dla $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $H = \{0, 2, 4, 6, 8\}$ jest podgrupą grupy \mathbb{Z}_{10} .

2.2 Generatory

$$\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$$

Grupa cykliczna, to grupa, która posiada co najmniej jednoelementowy zbiór generatorów. $\exists_{g \in G} \langle g \rangle = G$

2.3 Problem logarytmu dyskretnego

Niech $G = \langle g \rangle$. Problemem jest znalezienie x takiego, że $g^x = a$. W zależności od grupy oraz jej rozmiaru, ten problem może być niezwykle trudny.

2.4 Warstwy

Dla podgrupy H grupy G , warstwą lewostronną H wyznaczoną przez $a \in G$ jest zbiór:

$$\{a + H = \{a + h : h \in H\} \mid aH = \{ah : h \in H\}\}$$

Warstwy są identyczne, albo rozłączne. Suma mnogościowa warstw jest równa grupie G . Indeks podgrupy H w grupie G ($G : H$) nazywamy moc zbioru warstw względem podgrupy H .

$$G : H = \frac{|G|}{|H|}$$

Rząd podgrupy H jest dzielnikiem rzędu grupy G .

3 RSA

Asymetryczny algorytm szyfrujący, w którym każda strona ma parę kluczy: publiczny i prywatny. Enkrypcja odbywa się przy pomocy klucza publicznego drugiej strony, a dekrypcja przy pomocy klucza prywatnego.

3.1 Definicja

Dla danych liczb pierwszych p i q .

$$n = pq$$

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

Następnie wybieramy liczbę e względnie pierwszą z $\varphi(n)$. Klucz prywatny d musi spełniać warunek $ed \equiv 1 \pmod{\varphi(n)}$, zatem

$$d = e^{-1} \pmod{\varphi(n)}$$

(n, e) tworzy klucz publiczny, a (n, d) klucz prywatny.

Szyfrowanie wiadomości M odbywa się za pomocą wzoru:

$$C = M^e \pmod{n}$$

Odkrycie wiadomości M odbywa się za pomocą wzoru:

$$M = C^d \pmod{n}$$

3.2 Trudność problemu

Trudność wynika ze znalezienia $\varphi(n)$, a ponieważ weryfikacja czy znalezione $\varphi(n)$ jest poprawne wymaga zastosowania rozszerzonego algorytmu Euklidesa; odszyfrowanie wiadomości C wymaga znalezienia d .

3.3 Przykład

$$p = 7, q = 11 \Rightarrow n = 77, \varphi(n) = 60$$

$$e = 13 \Rightarrow d = 37 \Rightarrow \begin{cases} (n, e) = (77, 13) \\ (n, d) = (77, 37) \end{cases}$$

$$M = 15 \Rightarrow C = 15^{13} \pmod{77} = 64$$

$$C = 64 \Rightarrow M = 64^{37} \pmod{77} = 15$$