

Spis treści

1	Szyfr Shannona	1
1.1	Szyfr XOR	1
1.2	Bezpieczeństwo doskonałe	1
2	Struktury algebraiczne	2
2.1	Podgrupa	2
2.2	Generatory	2
2.3	Warstwy	2
3	Problemy	2
3.1	Problem logarytmu dyskretnego (DL)	2
3.2	Problem DDH	3
3.3	CDH	3
4	Schematy	3
4.1	Protokół DH	3
4.2	Schemat szyfrowania z kluczem publicznym	4
5	Ataki	4
5.1	Man-in-the-middle	4
5.2	Bezpieczeństwo semantyczne	4
5.3	Atak CDA	5
6	RSA	5
6.1	Definicja	5
6.2	Trudność problemu	5
6.3	Przykład	5

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:

$$\forall_{a,b \in H} a * b \in H$$

$$\forall_{a \in H} a^{-1} \in H$$

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 Warstwy

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

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

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 Problemy

3.1 Problem logarytmu dyskretnego (DL)

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.

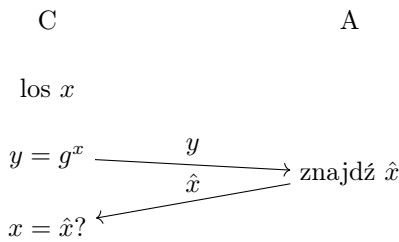


Diagram 1: Formalizm gry dla problemu logarytmu dyskretnego

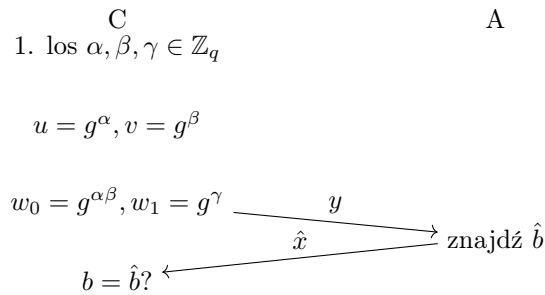


Diagram 2: Formalizm gry dla problemu DDH

3.2 Problem DDH

Mamy daną grupę cykliczną $G = \langle g \rangle$, rzędu q , gdzie q jest liczbą pierwszą. Losujemy $\alpha, \beta, \gamma \in \mathbb{Z}_q$. Następnie obliczamy:

$$u = g^\alpha, v = g^\beta, w_0 = g^{\alpha\beta}, w_1 = g^\gamma$$

Celem problemu, jest odgadnięcie b , dla danego u, v, w_b .

3.3 CDH

Mamy daną grupę cykliczną $G = \langle g \rangle$, rzędu q , gdzie q jest liczbą pierwszą. Losujemy $\alpha, \beta, \gamma \in \mathbb{Z}_q$. Następnie obliczamy:

$$u = g^\alpha, v = g^\beta, w = g^{\alpha\beta}$$

Celem problemu, jest odgadnięcie w , dla danego u, v .

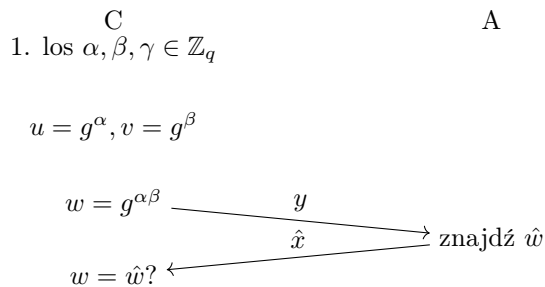


Diagram 3: Formalizm gry dla problemu CDH

4 Schematy

4.1 Protokół DH

Mamy daną grupę cykliczną $G = \langle g \rangle$, rzędu q , gdzie q jest liczbą pierwszą. Protokół Diffie-Hellman (DH), polega na losowym wybraniu sekretów przez dwóch użytkowników (A, B) $\alpha, \beta \in \mathbb{Z}_q$. Obliczeniu szyfrogramów $u = g^\alpha, v = g^\beta$,

a następnym wysłaniu u i v . Sekret wspólny $s = g^{\alpha\beta}$.

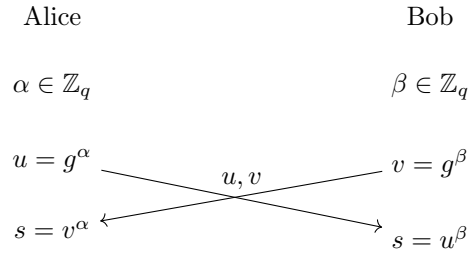


Diagram 4: Formalizm gry dla protokołu DH

Protokół jest odporny na atak pasywny (tylko czytanie). Z kolei, jest podatny na atak jeśli atakujący ma wpływ na kanał komunikacji, chociażby poprzez atak Man-in-the-middle.

4.2 Schemat szyfrowania z kluczem publicznym

$$\varepsilon = (G, E, D) \text{ nad } (M, C, K)$$

gdzie $G : \mathbb{N} \rightarrow K$, $E : K \times M \rightarrow C$, $D : K \times C \rightarrow M$.

$$(pk, sk) = G(\lambda)$$

$$C = E(pk, m)$$

$$M = D(sk, C)$$

5 Ataki

5.1 Man-in-the-middle

Jeśli atakujący ma wpływ na kanał komunikacji, to może przechwycić komunikaty podczas przekazywania kluczy. W takim momencie, może się podszyć pod drugą stronę, aby uzyskać dostęp do klucza prywatnego. Równocześnie może przekazywać dalej komunikację, aby ukryć swoją obecność. W ten sposób zna obydwa sekrety i tylko siedzi po środku.

5.2 Bezpieczeństwo semantyczne

Dla pewnego $\varepsilon = (G, E, D)$, atakujący ma dostęp do klucza publicznego pk . Wybiera on dwie wiadomości $m_0, m_1 \in M$. Przeciwnik wybiera jedną wiadomość $b \in \{0, 1\}$, szyfruje ją $c = E(pk, m_b)$ i zwraca atakującemu. Atakujący musi zgadnąć b .

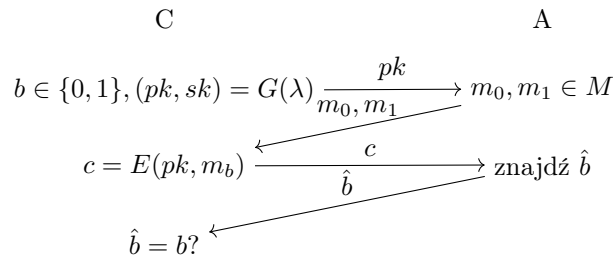


Diagram 5: Formalizm gry dla bezpieczeństwa semantycznego

5.3 Atak CDA

Jest to powielona wersja bezpieczeństwa semantycznego. Wielokrotnie atakujący może tworzyć wiadomości i dostawać losowy kryptogram na podstawie ich. To czyni ten atak o wiele trudniejszym niż bezpieczeństwo semantyczne.

6 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.

6.1 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:

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

6.2 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 .

6.3 Przykład

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

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

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

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