Spis treści

1 Złożoność obliczeniowa **1**
1.1 Dodawanie . . . 1
1.2 Mnożenie . . . 1
1.3 Potęgowanie . . . 1
1.4 Dzielenie . . . 1
1.5 Modulo . . . 2
1.6 Znajdowanie odwrotności . . . 2

2 Szyfr Shannona **2**
2.1 Szyfr XOR . . . 2
2.2 Bezpieczeństwo doskonałe . . . 2

3 Struktury algebraiczne **2**
3.1 Podgrupa . . . 3
3.2 Generatory . . . 3
3.3 Warstwy . . . 3
3.4 Homomorfizmy . . . 3

4 Problemy **3**
4.1 Problem logarytmu dyskretnego (DL) . . . 3
4.2 Problem DDH . . . 3
4.3 CDH . . . 4

5 Schematy **4**
5.1 Protokół DH . . . 4
5.2 Schemat szyfrowania z kluczem publicznym . . . 4

6 Ataki **5**
6.1 Man-in-the-middle . . . 5
6.2 Bezpieczeństwo semantyczne . . . 5
6.3 Atak CDA . . . 5

7 RSA **5**
7.1 Definicja . . . 6
7.2 Trudność problemu . . . 6
7.3 Przykład . . . 6

1 Złożoność obliczeniowa

1.1 Dodawanie

Dodanie dwóch liczb binarnych a i b o długości n ma złożoność $O(n)$, lub lepiej $O(\log \max(a, b))$.

1.2 Mnożenie

Mnożenie dwóch liczb binarnych a i b o długości n ma złożoność $O(n^2)$, lub lepiej $O(\log^2 \max(a, b))$.

1.3 Potęgowanie

Potęgowanie liczby a do potęgi b ma złożoność $O(\log^b a)$.

1.4 Dzielenie

Dzielenie liczby a przez b ma złożoność $O(n^2)$.

1.5 Modulo

Modulo liczby a przez b ma złożoność $O(n^2)$.

1.6 Znajdowanie odwrotności

To zależy od grupy, ale dla a w przypadku Z_n wymaga obliczenia $n - a$, czyli $O(\log \max(a, n))$. W przypadku $Z_n^\times$ wymaga użycia rozszerzonego algorytmu Euklidesa. Ten wykonuje w najgorszym przypadku a iteracji, więc złożoność wynosi $O(a \log^2 \max(a, n))$.

2 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:

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

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

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

2.1 Szyfr XOR

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

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

2.2 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 $|K| \geq |M|$.

3 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.

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

3.1 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 $\mathbb{Z}_{10}$.

3.2 Generatory

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

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

3.3 Warstwy

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

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

Warstwy są identyczne, albo rozłączne. Warstwy aH i bH są sobie równe kiedy $a^{-1}b \in H$. Suma mnogościowa warstw jest równa grupie G. Indeksem 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.

3.4 Homomorfizmy

$f : G \to G'$ nazywamy homomorfizmem grupy G w grupę G', jeśli zachodzi:

$$f(a + b) = f(a) + f(b)$$

$$f(ab) = f(a)f(b)$$

Jeśli:

- f jest iniekcją, to mówimy że f jest monomorfizmem.
- f jest suriekcją, to mówimy że f jest epimorfizmem.
- f jest bijekcją, to mówimy że f jest izomorfizmem.

Z własności homomorfizmu wynika, że $f(e) = f(ee) = f(e)f(e) = e'$ oraz $f(a^{-1}) = f(a)^{-1}$ i $f(a)f(a^{-1}) = f(e)$.
Zbiór $Ker(f) = \{a \in G : f(a) = e'\}$ nazywamy jądrem homomorfizmu f.
Zbiór $Im(f) = \{f(a) : a \in G\}$ nazywamy obrazem homomorfizmu f.

4 Problemy

4.1 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.

4.2 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.

C		A
los x		
$y = g^x$	$\xrightarrow{y}$	znajdź $\hat{x}$
$x = \hat{x}?$	$\xleftarrow{\hat{x}}$	

Diagram 1: Formalizm gry dla problemu logarytmu dyskretnego

C		A
1. los $\alpha, \beta, \gamma \in \mathbb{Z}_q$		
$u = g^{\alpha}, v = g^{\beta}$		
$w_0 = g^{\alpha\beta}, w_1 = g^{\gamma}$	$\xrightarrow{y}$	znajdź $\hat{b}$
$b = \hat{b}?$	$\xleftarrow{\hat{x}}$	

Diagram 2: Formalizm gry dla problemu DDH

4.3 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.

C		A
1. los $\alpha, \beta, \gamma \in \mathbb{Z}_q$		
$u = g^{\alpha}, v = g^{\beta}$		
$w = g^{\alpha\beta}$	$\xrightarrow{y}$	znajdź $\hat{w}$
$w = \hat{w}?$	$\xleftarrow{\hat{x}}$	

Diagram 3: Formalizm gry dla problemu CDH

5 Schematy

5.1 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 $s = g^{\alpha\beta}$.

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.

5.2 Schemat szyfrowania z kluczem publicznym

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

$$
\begin{tikzcd}
\text{Alice} & & \text{Bob} \\
\alpha \in \mathbb{Z}_q & & \beta \in \mathbb{Z}_q \\
u = g^{\alpha} \arrow[rrd] & u, v & v = g^{\beta} \arrow[lld] \\
s = v^{\alpha} & & s = u^{\beta}
\end{tikzcd}
$$

Diagram 4: Formalizm gry dla protokołu DH

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

$$
\begin{aligned}
(pk, sk) &= G(\lambda) \\
C &= E(pk, m) \\
M &= D(sk, C)
\end{aligned}
$$

6 Ataki

6.1 Man-in-the-middle

Jeśli atakujący ma wplyw 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.

6.2 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.

$$
\begin{tikzcd}
\text{C} & \text{A} \\
b \in \{0,1\}, (pk, sk) = G(\lambda) \arrow[r, "pk"] & m_0, m_1 \in M \arrow[dl, "m_0, m_1"'] \\
c = E(pk, m_b) \arrow[r, "c"] & \text{znajdź } \hat{b} \arrow[dl, "\hat{b}"'] \\
\hat{b} = b? &
\end{tikzcd}
$$

Diagram 5: Formalizm gry dla bezpieczeństwa semantycznego

6.3 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.

7 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.

7.1 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:

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

7.2 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.

7.3 Przykład

$$p = 7, q = 11 \Rightarrow n = 77, \varphi(n) = 60$$
$$e = 13 \Rightarrow d = 37 \Rightarrow \begin{cases} (n, e) = (77, 13) \\ (n, d) = (77, 37) \end{cases}$$
$$M = 15 \Rightarrow C = 15^{13} \pmod{77} = 64$$
$$C = 64 \Rightarrow M = 64^{37} \pmod{77} = 15$$