

WKR egzamin - Zakres materiału

Wstęp do kryptologii

Piotr Mroczkowski

WKR - zaliczenie przedmiotu

WKR - zaliczenie egzaminu

- Wprowadzenie do przedmiotu; notacja i pojęcia elementarne; bezpieczeństwo informacji: poufność, integralność, uwierzytelnienie, identyfikacja; definicja i własności kryptosystemu; zasada Kerckhoffsa; teoria liczb; algebra abstrakcyjna.
- Podział i rodzaje szyfrów; twierdzenie Shanonna; algorytm Euklidesa i rozszerzona jego postać; kodowanie alfabetu; obliczanie odwrotności multiplikatywnej; szyfr przesuwający; szyfr afiniczny; szyfr Vigenere'a; szyfr Hilla.
- Generator grupy multiplikatywnej; problemy teorii liczb w kryptografii: problem rozkładu liczby całkowitej na czynniki pierwsze, problem logarytmu dyskretnego, problem Diffie-Hellmana.

WKR egzamin - Zakres materiału

Wstęp do kryptologii

Piotr Mroczkowski

WKR - zaliczenie przedmiotu

WKR - zaliczenie egzaminu

I

- Kryptografia asymetryczna - idea i własności kryptosystemów klucza publicznego.
- Algorytm Diffie-Hellmana; bezpieczeństwo algorytmu DH: atak metodą „man in the middle”.
- Kryptosystem RSA: generacja kluczy, szyfrowanie/deszyfrowanie, generacja i weryfikacja podpisu cyfrowego; bezpieczeństwo kryptosystemu RSA.
- Kryptosystem ElGamala: generacja kluczy, szyfrowanie/deszyfrowanie, generacja i weryfikacja podpisu cyfrowego; bezpieczeństwo kryptosystemu ElGamala.

WKR egzamin - Zakres materiału

Wstęp do kryptologii

Piotr Mroczkowski

WKR - zaliczenie przedmiotu

WKR - zaliczenie egzaminu

- Szyfry strumieniowe – idea szyfrowania strumieniowego; liniowe rejesty przesuwające ze sprzężeniem zwrotnym - LFSR; generator z filtrem, generator kombinacyjny, złożoność liniowa, szyfr strumieniowy Trivium. I
- Szyfry blokowe – idea szyfrowania blokowego; architektury konstruowania szyfrów blokowych; szyfr blokowy DES; szyfr blokowy AES, tryby pracy szyfrów blokowych.
- Jednokierunkowe funkcje skrótu: klasyfikacja i własności, podstawowe struktury funkcji skrótu: model ogólny iteracyjnej funkcji skrótu, rodzina MD/SHA, funkcje skrótu wykorzystujące szyfry blokowe, konstrukcja gąbki; bezpieczeństwo funkcji skrótu: ataki ogólne (kolizje, pseudokolizje, atak na przeciwbraz), paradoks dnia urodzin, funkcja skrótu SHA-3.

Kryptologia - zastosowanie

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- 1 Zastosowania militarne (np. szyfratory)
- 2 Dyplomacja
- 3 Łączność
 - przewodowa (PSTN, ISDN, ...)
 - bezprzewodowa (GSM, SAT, Radio, WiFi, bluetooth, ...)
- 4 Bankowość elektroniczna
- 5 Protokoły internetowe (HTTPS, SSH, SSL - TLS, PGP, ...)
- 6 Motoryzacja i lotnictwo
- 7 Systemy uwierzytelnienia
- 8 Systemy dostępowe
- 9 Kryptowaluty - Bitcoin, Ethereum, Ripple, Litecoin, itd.
- 10 IoT
- 11 ...

Obecnie kryptografia stosowana jest do ochrony wszelkich danych cyfrowych we współczesnym świecie.

Teoria liczb

Wstęp do kriptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Niech \mathbb{Z} oznacza zbiór liczb całkowitych $\{\dots, -2, -1, 0, 1, 2, \dots\}$

Definicja

Niech $a, b \in \mathbb{Z}$ będą liczbami całkowitymi.

Liczba b dzieli a (b jest dzielnikiem a) jeśli istnieje liczba całkowita k taka, że $a = k * b$.

Jeśli b dzieli a , to jest to oznaczane jako $b|a$.

Przykład:

- $-3|18$, ponieważ istnieje liczba całkowita -6 taka, że $(-3) \cdot (-6) = 18$;
- $173|0$, ponieważ istnieje liczba całkowita 0 taka, że $173 \cdot 0 = 0$.

Teoria liczb

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Algorytm dzielenia liczb całkowitych

Jeśli $a \in \mathbb{Z}$ i $n \in \mathbb{N} - \{0\}$, to dzielenie całkowitoliczbowe a przez n daje w wyniku liczbę całkowitą q (część całkowita dzielenia) oraz resztę r (reszta dzielenia) takie że:

$$a = qn + r$$

przy czym $0 \leq r < n$.

Przykład:

Niech $a = 73$ i $n = 17$, to:

$$q = 73 \text{ div } 17 = 4$$

$$r = 73 \text{ mod } 17 = 5.$$

Teoria liczb

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Definicja

Liczba całkowita d jest wspólnym dzielnikiem liczb a i b wówczas, gdy $d|a$ oraz $d|b$.

Definicja

Największym wspólnym dzielnikiem liczb całkowitoliczbowych a i b , nazywa się taką nieujemną liczbę d , oznaczaną $d = \gcd(a, b)$ ($d = \text{nwd}(a, b)$), która jest wspólnym dzielnikiem liczb a oraz b , a przy tym każdy wspólny dzielnik a i b dzieli d .

Symbolicznie można to wyrazić następująco: $d = \gcd(a, b)$, gdy:

- 1 $d|a$ i $d|b$,
- 2 jeśli $c|a$ i $c|b$, to $c|d$ dla dowolnej liczby c .

Teoria liczb

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Definicja

Dwie liczby całkowite $a, b \in \mathbb{Z}$ są względnie pierwsze wówczas, gdy $\gcd(a, b) = 1$.

Szybkim sposobem określenia, czy dwie liczby są względnie pierwsze jest algorytm Euklidesa.



Przykłady:

- liczby 6 i 35 są względnie pierwsze, ale 6 i 27 nie są, gdyż obie są podzielne przez 3,
- liczba 1 jest względnie pierwsza z każdą liczbą całkowitą,
- liczby 10, 12 i 15 są względnie pierwsze, ale nie są parami względnie pierwsze.

Kongruencje

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Niech:

$n \in N$ będzie liczbą naturalną bez zera;
 $a, b \in Z$ będą liczbami całkowitymi.

Definicja

Liczba a jest **kongruentna do b** (a przystaje do b) modulo n , co zapisujemy $a \equiv b \text{ mod } n$, jeśli $n|(a - b)$.

Liczbe n nazywamy modułem kongruencji.

Przykład:

- $24 \equiv 9 \text{ mod } 5$, ponieważ $5|(24 - 9)$,
- $23 \equiv -5 \text{ mod } 7$, ponieważ $7|(23 - (-5))$,
- $-5 \equiv 4 \text{ mod } 3$, ponieważ $3|(-5 - 4)$.

Odwrotność multiplikatywna

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Definicja

Odwrotnością multiplikatywną a modulo n nazywamy liczbę całkowitą $a^{-1} \in Z_n$ taką, że $a \cdot a^{-1} \equiv 1 \pmod{n}$.

Jeśli takie a^{-1} istnieje, to mówimy, że a jest odwracalne.

I

Teoria liczb

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Definicja

Liczba całkowita d jest wspólnym dzielnikiem liczb a i b wówczas, gdy $d|a$ oraz $d|b$.

Definicja

Największym wspólnym dzielnikiem liczb całkowitoliczbowych a i b , nazywa się taką nieujemną liczbę d , oznaczaną $d = \gcd(a, b)$ ($d = \text{nwd}(a, b)$), która jest wspólnym dzielnikiem liczb a oraz b , a przy tym każdy wspólny dzielnik a i b dzieli d .

Symbolicznie można to wyrazić następująco: $d = \gcd(a, b)$, gdy:

- 1 $d|a$ i $d|b$,
- 2 jeśli $c|a$ i $c|b$, to $c|d$ dla dowolnej liczby c .

Przykład:

Wspólnymi dzielnikami liczb 12 i 18 są $\{\pm 1, \pm 2, \pm 3, \pm 6\}$.

Największy wspólny dzielnik liczb 12 i 18: $\gcd(12, 18) = 6$.

Teoria liczb

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Algorytm dzielenia liczb całkowitych

Jeśli $a \in \mathbb{Z}$ i $n \in \mathbb{N} - \{0\}$, to dzielenie całkowitoliczbowe a przez n daje w wyniku liczbę całkowitą q (*część całkowita dzielenia*) oraz resztę r (*reszta dzielenia*) takie że:

$$a = qn + r$$

przy czym $0 \leq r < n$.

Odwrotność multiplikatywna

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - chemiczno-tytu

Podsumowanie

Definicja

Odwrotnością multiplikatywną a modulo n nazywamy liczbę całkowitą $a^{-1} \in Z_n$ taką, że $a \cdot a^{-1} \equiv 1 \pmod{n}$.

Jeśli takie a^{-1} istnieje, to mówimy, że a jest odwracalne.

Teoria liczb

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy

matematyczne

Szłyby - charakterystyka

Podsumowanie

Definicja

Liczba całkowita d jest wspólnym dzielnikiem liczb a i b wówczas, gdy $d|a$ oraz $d|b$.

Definicja



Największym wspólnym dzielnikiem liczb całkowitoliczbowych a i b , nazywa się taką nieujemną liczbę d , oznaczaną $d = \gcd(a, b)$ ($d = \text{nwd}(a, b)$), która jest wspólnym dzielnikiem liczb a oraz b , a przy tym każdy wspólny dzielnik a i b dzieli d .

Symbolicznie można to wyrazić następująco: $d = \gcd(a, b)$, gdy:

- 1 $d|a$ i $d|b$,
- 2 jeśli $c|a$ i $c|b$, to $c|d$ dla dowolnej liczby c .

Definicja

Dwie liczby całkowite $a, b \in \mathbb{Z}$ są względnie pierwsze wówczas, gdy $\gcd(a, b) = 1$.

Szybkim sposobem określenia, czy dwie liczby są względnie pierwsze jest algorytm Euklidesa.



Przykłady:

- liczby 6 i 35 są względnie pierwsze, ale 6 i 27 nie są, gdyż obie są podzielne przez 3,
- liczba 1 jest względnie pierwsza z każdą liczbą całkowitą,
- liczby 10, 12 i 15 są względnie pierwsze, ale nie są parami względnie pierwsze.

Dodawanie, odejmowanie, mnożenie modularne

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Niech $Z_n = \{0, 1, 2, \dots, n-1\}$ - oznacza zbiór liczb całkowitych modulo n .

Definicja

Dodawanie, odejmowanie, mnożenie w Z_n są wykonywane modulo n .

I

Przykład:

$$Z_{25} = \{0, 1, 2, \dots, 24\}.$$

$$(13 + 16) \bmod 25 = 29 \bmod 25 = 4$$

$$(13 - 16) \bmod 25 = -3 \bmod 25 = 22$$

$$(13 \cdot 16) \bmod 25 = 208 \bmod 25 = 8.$$

Arytmetyka modularna w Z_n

- 1 dodawanie jest zamknięte: $a, b \in Z_n, a + b \in Z_n$;
- 2 dodawanie jest przemienne: $a, b \in Z_n, a + b = b + a$;
- 3 dodawanie jest łączne: dla $a, b, c \in Z_n, (a + b) + c = a + (b + c)$;
- 4 zero jest elementem neutralnym względem dodawania:
 $a \in Z_n, a + 0 = 0 + a = a$;
- 5 elementem przeciwnym do $a \in Z_n$ jest $n - a$:
 $a + (n - a) = (n - a) + a = 0$;
- 6 mnożenie jest zamknięte: $a, b \in Z_n, ab \in Z_n$;
- 7 mnożenie jest przemienne: $a, b \in Z_n, ab = ba$;
- 8 mnożenie jest łączne: $a, b, c \in Z_n, a(bc) = (ab)c$;
- 9 jedynka jest elementem neutralnym względem mnożenia:
 $a \in Z_n, 1a = a1 = a$;
- 10 elementem odwrotnym do $a \in Z_n$ jest $a^{-1} \in Z_n$ taki, że
 $a \cdot a^{-1} \equiv 1 \pmod{n}$;
- 11 dodawanie i mnożenie są działaniami rozdzielnymi: $a, b, c \in Z_n$,
 $(a + b)c = ac + bc, a(b + c) = ab + ac$.

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Grupy, pierścienie, ciała

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Definicja

Zbiór Z_n z operacją dodawania tworzy strukturę algebraiczną zwaną grupą przemienną (abelową).

Definicja

Zbiór Z_n z operacją dodawania i mnożenia jest pierścieniem przemiennym.

Definicja

Jeżeli dla każdego $a \in Z_n - \{0\}$ istnieje element odwrotny $a^{-1} \in Z_n$ to taki pierścień nazywamy ciałem.



Grupy, pierścienie, ciała

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykłada

Podstawowe pojęcia i tematyki

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Przykład:

Niech $n = 5$, wówczas $Z_5 = \{0, 1, 2, 3, 4\}$.

Działania dodawania i mnożenia w Z_5 :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

*	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Pierścień Z_5 jest ciałem, ponieważ każdy niezerowy element pierścienia jest odwracalny.

Arytmetyka modularna w Z_n

Wstęp do kriptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- 1 dodawanie jest zamknięte: $a, b \in Z_n, a + b \in Z_n$;
- 2 dodawanie jest przemienne: $a, b \in Z_n, a + b = b + a$;
- 3 dodawanie jest łączne: dla $a, b, c \in Z_n, (a + b) + c = a + (b + c)$;
- 4 zero jest elementem neutralnym względem dodawania:
 $a \in Z_n, a + 0 = 0 + a = a$;
- 5 elementem przeciwnym do $a \in Z_n$ jest $n - a$:
 $a + (n - a) = (n - a) + a = 0$;
- 6 mnożenie jest zamknięte: $a, b \in Z_n, ab \in Z_n$;
- 7 mnożenie jest przemienne: $a, b \in Z_n, ab = ba$;
- 8 mnożenie jest łączne: $a, b, c \in Z_n, a(bc) = (ab)c$;
- 9 jedynka jest elementem neutralnym względem mnożenia:
 $a \in Z_n, 1a = a1 = a$;
- 10 elementem odwrotnym do $a \in Z_n$ jest $a^{-1} \in Z_n$ taki, że
 $a \cdot a^{-1} \equiv 1 \pmod{n}$;
- 11 dodawanie i mnożenie są działaniami rozdzielnymi: $a, b, c \in Z_n, (a + b)c = ac + bc, a(b + c) = ab + ac$.

Literatura

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

■ Literatura podstawowa:

- 1 William Stallings: "Kryptografia i bezpieczeństwo w sieciach komputerowych. Matematyka szyfrów szyfrów i techniki kryptologii"
- 2 William Stallings: "Kryptografia i bezpieczeństwo w sieciach komputerowych. Koncepcje i metody bezpiecznej komunikacji"
- 3 Alfred J. Menezes: "Handbook of Applied Cryptography"
- 4 Jean Philippe Aumasson: "Nowoczesna kryptografia. Praktyczne wprowadzenie do szyfrowania"

■ Literatura uzupełniająca:

- 1 R. Stinson: "Cryptography"
- 2 B. Schneier: "Kryptografia dla praktyków"

Grupy dyskusyjne i fora internetowe

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- **sci.crypt.research** - grupa poświęcona badaniom naukowym z dziedziny kryptologii
- **sci.crypt** - dyskusje związane z wszelkimi aspektami kryptologii
- **alt.security** - forum dyskusji na temat ogólnie pojętego bezpieczeństwa w informatyce
- **comp.security.misc** - forum dyskusyjne na temat bezpieczeństwa użytkowania komputerów
- **fgrum Security and Cryptography** w witrynie devshed.com - dyskusje nt. ogólnie pojętego bezpieczeństwa i kryptografii
- **forum Cryptography** w witrynie topix.com - dyskusje są ściśle zorientowane na techniczne aspekty kryptografii

Standardy dot. kryptologii

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- 1 NIST (National Institute of Standards and Technology)** - Narodowy Instytut Standaryzacji Technologii Stanów Zjednoczonych - agencja federalna USA zajmująca się teorią i praktyką miar i pomiarów, standardów oraz technologii wykorzystywanych w administracji państowej i cywilnych agencjach rządowych. Publikowane przez NIST standardy:
 - **FIPS (Federal Information Processing Standard)** - federalny standard przetwarzania informacji,
 - **SP (Special Publications)** - publikacje specjalne, mają zasięg ogólnowiatowy.
- 2 ISO (International Organization for Standardization)** - Międzynarodowa Organizacja Normalizacyjna będąca pozarządową organizacją zrzeszającą krajowe organizacje normalizacyjne (m.in. PKN).
- 3 PKN (Polski Komitet Normalizacyjny)**

Plan wykładu

Wstęp do kriptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

1 Podstawowe pojęcia i terminy

2 Podstawy matematyczne

- teoria liczb
- kongruencje
- algebra abstrakcyjna

3 Szyfry - charakterystyka

- szyfry monoalfabetyczne, szyfry polialfabetyczne
- szyfry przestawieniowe, szyfry podstawieniowe
- szyfry współczesne

4 Podsumowanie

Zagrożenia dla bezpieczeństwa informacji

Wstęp do kryptografii

Piotr

Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

1 Podśluch:

- zdobycie informacji przechowywanych na stanowisku komputerowym
- zdobycie informacji przesyłanych w sieci
- poznanie protokołów wymiany danych
- poznanie protokołów kryptograficznych

2 Ataki na integralność

- 3 Nieuprawniony dostęp do zasobów sieci
- 4 Nieuprawnione działania legalnego użytkownika
- 5 Zaprzeczenie: nadania, odbioru, treści informacji
- 6 Maskarada (masquerade) - polega na podszywaniu się pod legalnego użytkownika.
- 7 Odmowa usługi (Denial of service) - to niemożność korzystania z usługi przez uprawnionych do tego użytkowników.
- 8 Generowanie sztucznego ruchu
- 9 Powtórzenia (replay) - polega na pasywnym przechwyceniu porcji danych i ich retransmisji w celu otrzymania niedozwolonych rezultatów.

Zagrożenia dla bezpieczeństwa informacji - przykłady

Wstęp do kryptografii

Piotr

Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- 1 Główny księgowy przesyła prezesowi plik zawierający poufną informację (np. listę płac w firmie) i jego zawartość absolutnie nie może dostać się w niepowołane ręce. Niestety pracownik Xsiński, przed którym informacja powinna być ukryta, uzyskuje możliwość monitorowania transmisji i uzyskuje kopię tego pliku.
- 2 Prezes przesyła Głównemu Księgowemu poufną informację zwrotną (np. zmodyfikowaną listę płac). Xsiński, który ma możliwość monitorowania transmisji przechwytuje plik, modyfikuje jego zawartość i przesyła zmienioną jego postać do Głównego Księgowego.
- 3 Administrator sieci chce nadać nowym użytkownikom nowe (zmodyfikować istniejące) uprawnienia w sieci. W tym celu przesyła do zarządzanego przez siebie serwera nową listę konfiguracyjną danych uwierzytelniających użytkowników. Użytkownik Xsiński przechwytuje plik konfiguracyjny, modyfikuje go według swoich potrzeb i przesyła do serwera. Serwer aktualnia uprawnienia użytkowników traktując przesłany plik konfiguracyjny jakby został wysłany przez Administratőra.

Zagrożenia dla bezpieczeństwa informacji - przykłady c.d.

Wstęp do kryptografii

Piotr

Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- 1 Xsiński zostaje zwolniony z firmy, w związku z czym kierownik działu kadr wysyła do firmowego serwera komunikat nakazujący usunięcie konta Xsińskiemu, które ma zostać potwierdzone przez serwer za pomocą odpowiedniego komunikatu. Xsiński ma możliwość przechwycenia komunikatu przesyłanego do serwera i chwilowego powstrzymania jego przesłania, dzięki czemu zyskuje czas, aby wykraść z serwera poufne informacje firmy. Następnie uwalnia przechwycony komunikat, który dociera do serwera. Serwer kasuje konto Xsińskiego i przesyła o tym komunikat zwrotny. Cała akcja może pozostać długo (być może na zawsze) niezauważona.
- 2 Klient przesyła maklerowi zlecenie kupna dużego pakietu akcji firmy X. Makler kupuje akcje, które zaczynają gwałtownie tracić na wartości, ale klient wypiera się wystawionego zlecenia zakupu.

Środki bezpieczeństwa

- Prawne: ustawy, kodeks karny
- Administracyjno-organizacyjne
 - 1 osoby odpowiedzialne za bezpieczeństwo
 - 2 przepisy i regulaminy postępowania
 - 3 uprawnienia
 - 4 szkolenia
- Fizyczne: kraty, zamki, sejfy, kabiny ekranujące, systemy alarmowe i ppoż.
- Techniczne
 - 1 ochrona dostępu (hasła, uprawnienia)
 - 2 przepisy i regulaminy postępowania
 - 3 ochrona antywirusowa
 - 4 kryptograficzne metody ochrony informacji
 - 5 steganograficzne metody ochrony informacji



Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Kryptologia - co to takiego?

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- 1 Kryptologia jest nauką ścisłą, zajmującą się praktycznym zastosowaniem matematyki w ochronie danych.
- 2 Kryptologia zajmuje się utajnionym zapisem danych.
- 3 Kryptologia - nauka o przekazywaniu informacji w sposób zabezpieczony przed niepowołanym dostępem.
- 4 Kryptologia jest nauką o szyfrowaniu, czyli bezpiecznych sposobach przekazywania informacji.
- 5 Kryptologia jest to proces przekształcania danych (tekstu jawnego) w szyfrogram (kryptogram, tekst zaszyfrowany) za pomocą odpowiedniego algorytmu kryptograficznego.
I
- 6 ...
- 7 Kryptologia - nauka obejmująca kryptografię i kryptoanalizę.

Kryptologia, kryptoanaliza

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Kryptologia = kryptografia + kryptoanaliza

- Kryptografia - dziedzina wiedzy i badań zajmująca się tworzeniem nowych algorytmów kryptograficznych:
 - szyfrów blokowych,
 - szyfrów strumieniowych,
 - funkcji skrótu,
 - algorytmów uwierzytelnionego szyfrowania,
 - algorytmów szyfrowania / dešzyfrowania kryptografii asymetrycznej,
 - algorytmów generacji / weryfikacji podpisu cyfrowego,
 - algorytmów uwierzytelnionego szyfrowania,
 -
- Kryptoanaliza - dziedzina wiedzy i badań zajmująca się łamaniem istniejących algorytmów kryptograficznych.

Cele kryptografii - atrybuty ochrony informacji

Wstęp do
kryptografii

Piotr
Mroczkowski

Wprowadzenie
do przedmiotu

Plan wykładu

Podstawowe
pojęcia i terminy

Podstawy
matematyczne

Szyfry -
charakterystyka

Podsumowanie

- Poufność (Confidentiality)
- Integralność danych (Data integrity)
- Uwierzytelnienie (Authentication)
- Niezaprzeczalność (Non-repudiation)

Atrybuty ochrony informacji

Wstęp do kryptografii

Piotr

Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

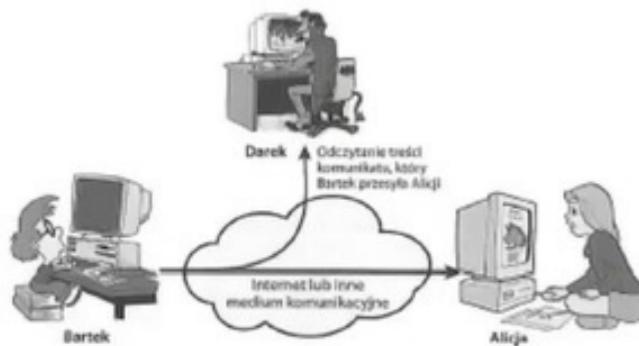
Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- Poufność – zabezpieczenie przed ujawnieniem treści informacji (danych).



Atrybuty ochrony informacji

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

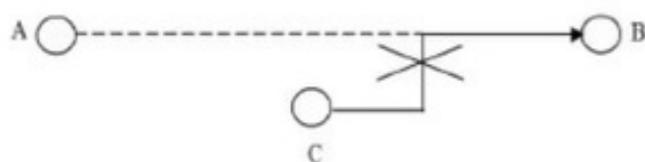
Podstawy matematyczne

Szyfry - charakterystyka

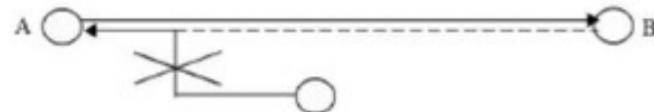
Podsumowanie

- **Uwierzytelnienie** – umożliwia: weryfikację autentyczności informacji (danych), potwierdzenie tożsamości nadawców, odbiorców informacji (danych), :

Nadawcy



Odbiorcy



Kryptologia - zastosowanie

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- 1** Zastosowania militarnie (np. szyfratory)
- 2** Dyplomacja
- 3** Łączność
 - przewodowa (PSTN, ISDN, ...)
 - bezprzewodowa (GSM, SAT, Radio, WiFi, bluetooth, ...)
- 4** Bankowość elektroniczna
- 5** Protokoły internetowe (HTTPS, SSH, SSL - TLS, PGP, ...)
- 6** Motoryzacja i lotnictwo
- 7** Systemy uwierzytelnienia
- 8** Systemy dostępowe
- 9** Kryptowaluty - Bitcoin, Ethereum, Ripple, Litecoin, itd.
- 10** IoT
- 11** ...

Obecnie kryptografia stosowana jest do ochrony wszelkich danych cyfrowych we współczesnym świecie.

Kamienie milowe kryptologii

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Okres	I w. p.n.e	Kryptografia	Kryptoanaliza	
			Okres	Opis
klasyczne szyfry ręczne	1 w. p.n.e	szыfr Cezara		
		szłyf podstawieniowe, przestawieniowe, polialfabetyczne wędrującego klucza	1863	złamanie szyfru polialfabetycznego
	1919	maszyny rotorowe Enigma	1890	złamanie szyfru wędrującego klucza
	1926	szłyf Vernama z kluczem jednorazowym	1933	złamanie szyfru Enigmy
	1949	Shannon – Communication Theory of Secrecy Systems	1945	złamanie szyfru purpurowego
	1976	Diffie, Hellman – New Directions in Cryptography		
	1977	DES – Data Encryption Standard		
	1978	RSA – szłyf z kluczem publicznym		
	1994	DSS – Digital Signature Standard		
	2000	AES – Advanced Encryption Standard (1997 - 2001)	1982	złamanie szłyfów plecakowego
szyfry maszynowe	2002	SHA-0 (1993), SHA-1 (1995), SHA-2 (2002)	1990	kryptoanaliza różnicowa
	2008	eSTREAM (2004-2008)	1993	kryptoanaliza liniowa
	2013	SHA-3 (2009-2012)	2000	faktoryzacja 512-bitowej liczby modularnej RSA
	2019	CESAR (2012-2019)		
	II faza	Post Quantum Cryptography (2016 - obecnie)	2004	kryptoanaliza f. skrótu MD, SHA-0, SHA-1

Kryptograficzne metody ochrony informacji

Wstęp do kryptografii

Piotr
Mroczkowski

Wprowadzenie
do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy
matematyczne

Szyfry - charakterystyka



- „Encryption works. Properly implemented strong cryptosystems are one of the few thinks that you can rely on” - Edward Snowden

Schemat komunikacji

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

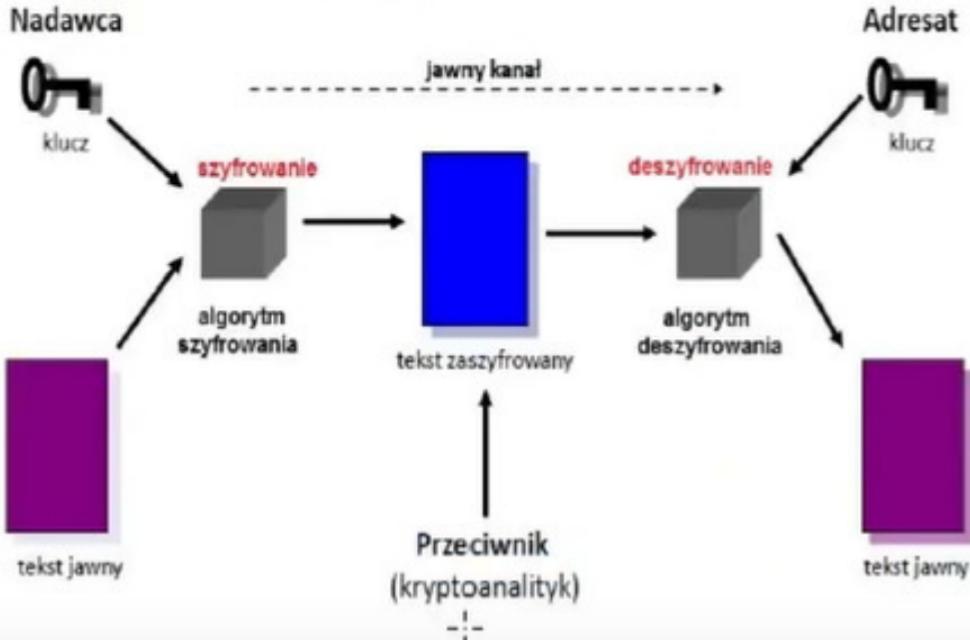
Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Schemat komunikacji



Realizacja usług ochrony informacji

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

1 Poufność

- kryptosystemy symetryczne
- kryptosystemy asymetryczne

2 Integralność

- CRC (Cyclic Redundancy Codes) - suma kontrolna
- kody korekcyjno-detekcyjne
- funkcje skrótu (Hash Functions)
- MAC (Message Authentication Codes)

3 Uwierzytelnienie

- kryptosystemy asymetryczne

4 Poufność, integralność i uwierzytelnienie

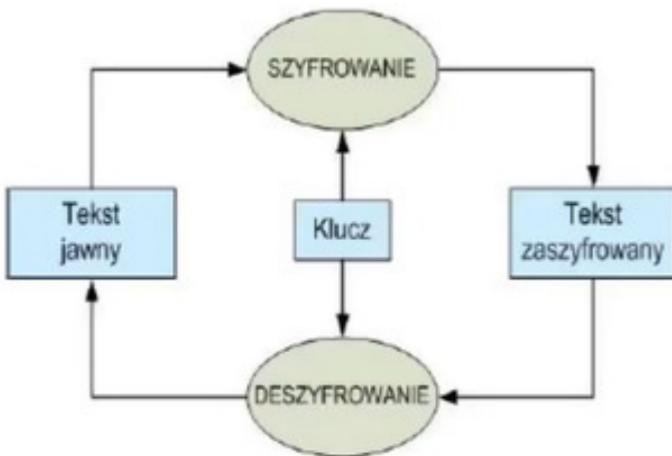
- uwierzytelnione szyfrowanie (Authenticated Encryption)

5 Niezaprzeczalność

- podpis cyfrowy



Usługa poufności



- **Tekst jawnny** - informacja (np. tekst w określonym języku, dane numeryczne, dźwięk, obraz, itp.), która nie została zaszyfrowana.
 - **Tekst zaszyfrowany** (szyfrogram, kryptogram) - informacja, która została zaszyfrowana.

Usługa poufności

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- **Szyfrowanie** – proces przekształcenia tekstu jawnego w tekst zaszyfrowany przy użyciu klucza szyfrowania, odbywający się według algorytmu szyfrowania.
- **Deszyfrowanie** - proces przekształcenia tekstu zaszyfrowanego w tekst jawnego przy użyciu klucza deszyfrowania, odbywający się według algorytmu deszyfrowania.
- **Szyfr** - funkcja matematyczna wykorzystywana do szyfrowania/deszyfrowania informacji z wykorzystaniem klucza szyfrowania/deszyfrowania składająca się z:
 - algorytmu szyfrowania,
 - algorytmu deszyfrowania,
 - algorytmu generacji podklucza z klucza głównego.

Zazwyczaj jedna funkcja wykorzystywana jest do szyfrowania, a inna do deszyfrowania wiadomości.

Definicja kryptosystemu

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Kryptosystem to dowolna piątka (P, C, K, E, D) , gdzie:

- (P) - skończony zbiór tekstów jawnych;
 - (C) - skończony zbiór tekstów zaszyfrowanych;
 - (K) - skończony zbiór kluczy (przestrzeń klucza);
 - (E, D) - zbiory reguł odpowiednio szyfrowania: $e_k \in E$ oraz deszyfrowania $d_k \in D$;
 - Dla każdego $k \in K$:
 - 1 $e_k : P \rightarrow C$ - algorytm szyfrowania,
 - 2 $d_k : C \rightarrow P$ - algorytm deszyfrowania,
- spełniające warunek:

$$d_k(e_k(x)) = x$$

dla każdego $x \in P$, $k \in K$.

Właściwości kryptosystemu

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

System kryptograficzny musi spełniać trzy podstawowe warunki:

- 1 przekształcenia szyfrujące i deszyfrujące muszą być wzajemnie odwrotne,
- 2 przekształcenia szyfrujące i deszyfrujące muszą być efektywne dla wszystkich kluczy,
- 3 bezpieczeństwo kryptosystemu powinno zależeć tylko od poufności kluczy i nie zależeć od znajomoci algorytmu - zasada Kerckhoffsa.

Zasada Kerckhoffsa (1833r.)

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Zasada Kerckhoffsa

Algorytmy kryptograficzne (szyfrowania i deszyfrowania) są jawne, natomiast ich bezpieczeństwo opiera się na tajności kluczy.

Zasada ta obowiązuje w komercyjnych zastosowaniach kryptografii i oznacza, że:

- algorytmy kryptograficzne są jawne (kryptoanalityk zna specyfikację algorytmu);
- klucze są tajne (kryptoanalityk nie zna klucza deszyfrowania).

Teoria liczb

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Niech Z oznacza zbiór liczb całkowitych $\{\dots, -2, -1, 0, 1, 2, \dots\}$

Definicja

Niech $a, b \in Z$ będą liczbami całkowitymi.

Liczba b dzieli a (b jest dzielnikiem a) jeśli istnieje liczba całkowita k taka, że $a = k * b$.

Jeśli b dzieli a , to jest to oznaczane jako $b|a$.

Algorytm Euklidesa, 300 r.p.n.e.

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Dane wejściowe: dwie nieujemne liczby całkowite $a, b \in \mathbb{Z}^+$, $a \geq b$.

Dane wyjściowe: największy wspólny dzielnik: $d = \gcd(a, b)$.

- 1** Jeżeli $b = 0$ to $d \leftarrow a$, zwróć d ; I
- 2** Podziel a przez b otrzymując:
 - cześć całkowitą dzielenia: $q = a \text{ div } b$;
 - resztę dzielenia: $r = a \text{ mod } b$takie, że $a = q \cdot b + r$.
- 3** Jeżeli $r = 0$ to $d \leftarrow b$, zwróć d ,
w p.p. podstaw $a \leftarrow b$, $b \leftarrow r$ i idź do pkt. 2;

Teoria liczb

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Podstawowe twierdzenie arytmetyki

Każdą liczbę całkowitą $n \geq 2$ można rozłożyć na czynniki będące potęgami liczb pierwszych:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} = \prod_{i=1}^k p_i^{e_i}$$

gdzie: p_i - są różnymi liczbami pierwszymi,
 e_i - są dodatnimi liczbami całkowitymi określającymi liczbę powtórzeń p_i w rozkładzie.

Teoria liczb

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Definicja

Niech $n \geq 1$.

Funkcję $\varphi(n)$, oznaczającą ilość liczb całkowitych w przedziale $[1, n]$ które są względnie pierwsze z n , nazywamy **funkcją Eulera**.

Funkcja Eulera dana jest dla każdej liczby naturalnej n wzorem:

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

gdzie p_1, p_2, \dots, p_k są wszystkimi czynnikami pierwszymi liczby n licznymi bez powtórzeń.

Teoria liczb

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Własności funkcji Eulera:

- Funkcja Eulera jest multplikatywna, tzn. jeśli $\gcd(m, n) = 1$, to $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.
- Jeśli p jest liczbą pierwszą, to $\varphi(p) = p - 1$.
- Jeśli $n = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$ jest rozkładem na czynniki pierwsze liczby n , to:

$$\varphi(n) = \prod_{i=1}^k p_i^{e_i-1} \cdot (p_i - 1)$$

Przykład:

Niech: $p = 13$.
 $\varphi(13) = 13 - 1 = 12$

Niech: $n = 24 = 2^3 \cdot 3^1$.
 $\varphi(24) =$
 $2^{3-1} \cdot (2 - 1) \cdot 3^0 \cdot (3 - 1) = 8$

Kongruencje

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry – charakterystyka

Podsumowanie

Niech:

$n \in \mathbb{N}$ będzie liczbą naturalną bez zera;
 $a, b \in \mathbb{Z}$ będą liczbami całkowitymi.

Definicja

Liczba a jest **kongruentna** do b (a przystaje do b) modulo n , co zapisujemy $a \equiv b \pmod{n}$ jeśli $n|(a - b)$.

Liczبę n nazywamy modułem kongruencji.

Przykład:

- $24 \equiv 9 \pmod{5}$, ponieważ $5|(24 - 9)$,
- $23 \equiv -5 \pmod{7}$, ponieważ $7|(23 - (-5))$,
- $-5 \equiv 4 \pmod{3}$, ponieważ $3|(-5 - 4)$.

Podział szyfrów

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Szyfry dzielimy na:

- monoalfabetyczne - szyfr, w którym każdy ze znaków tekstu jawnego przekształcany jest zawsze na taki sam znak szyfrogramu;
- polialfabetyczne - szyfr, w którym każdy ze znaków tekstu jawnego może być przekształcany na różne znaki szyfrogramu.

Rodzaje szyfrów

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- Szyfry przestawieniowe - zmieniają uporządkowanie bloków danych (znaków, bitów) wg. ustalonej reguły (klucza).
 - szyfr płotowy,
 - scytale;

Szyfry przestawieniowe są łatwe do złamania i nie zapewniają żadnego bezpieczeństwa.



Szyfr płotowy

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Przykład:

tekst jawnny = KRYPTOGRAFIA

klucz = „4” (wysokość płotka)

K					G			
	R			O	R			A
-:-	Y	T			A	I		
		P				F		

tekst zaszyfrowany = KGRORAYTAIPF

Rodzaje szyfrów

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

- Szyfry przestawieniowe - zmieniają uporządkowanie bloków danych (znaków, bitów) wg. ustalonej reguły (klucza).
 - szyfr półowy,
 - scytale;

Szyfry przestawieniowe są łatwe do złamania i nie zapewniają żadnego bezpieczeństwa.
- Szyfry podstawienniowe - bloki danych (znaki, bity) zastępowane są innymi blokami danych wg. ustalonej reguły (klucza).
 - dysk szyfrowy,
 - szyfr Cezara;

Ze względu na łatwość łamania tego rodzaju szyfrów, nie są one już stosowane.
- Szyfry podstawiennowo - przestawieniowe - szyfry w których zastosowano podstawienia i przestawienia bloków danych (znaków, bitów) w wielokrotnie wykonywanej rundzie.

Szyfr Cesara

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

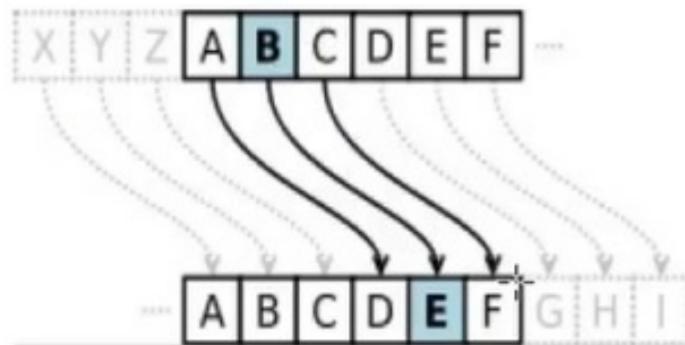
Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie



- Przykład:
tekst jawnny: warszawa

PT	w	a	r	s	z	a	w	a
CT	Z	D	U	V	C	D	Z	D

tekst zaszyfrowany: ZDUVCDZD

Szachownica Polibiusza

Wstęp do kryptografii

Piotr

Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Szachownica Polibiusza

rodzaj szyfru monoalfabetycznego wymyślony w starożytności przez greckiego historyka Polibiusza w którym każdej literze przypisana jest odpowiednia liczba, według następującej tabeli:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJK	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Cyfry oznaczają położenie danej litery w tabeli – pierwszą cyfrą jest numer wiersza, a drugą – kolumny.

Przykład: tekst jawnny: "tajne"

PT	t	a	j	n	e
CT	44	11	24	33	15

Scytale

Wstęp do
kryptografii

Piotr
Mroczkowski

Wprowadzenie
do przedmiotu

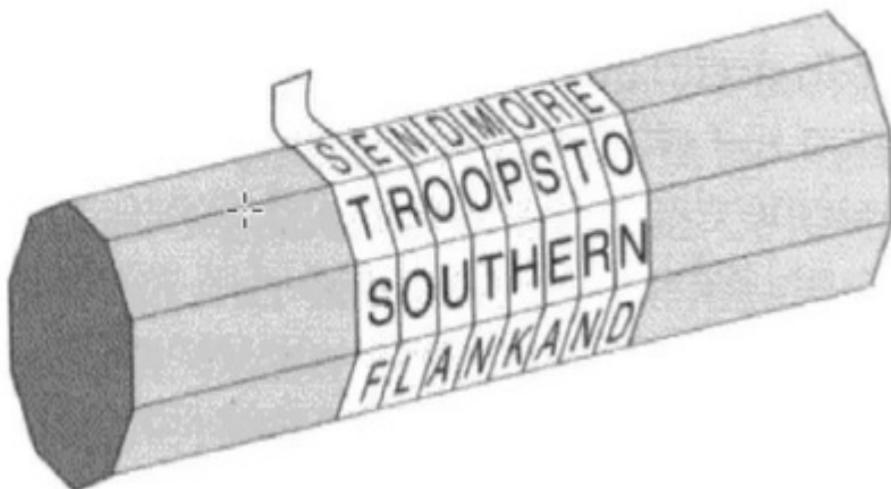
Plan wykładu

Podstawowe
pojęcia i terminy

Podstawy
matematyczne

Szyfry -
charakterystyka

Podsumowanie



Dysk szyfrowy

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

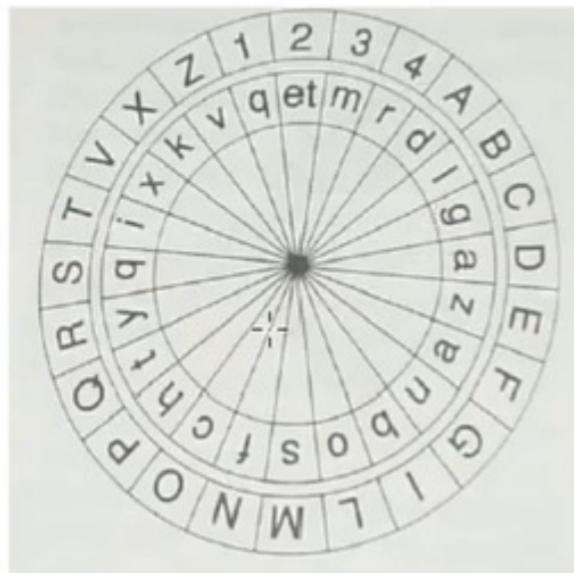
Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie



Enigma

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie



Szyfry współczesne

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Szyfrowanie symetryczne (systemy z kluczem tajnym):

- tajne klucze służą do szyfrowania i deszyfrowania informacji,
- klucz musi być dystrybuowany kanałem chronionym,
- klucz musi być chroniony w czasie użytkowania.

I

Szyfry współczesne - kryptosystemy symetryczne

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

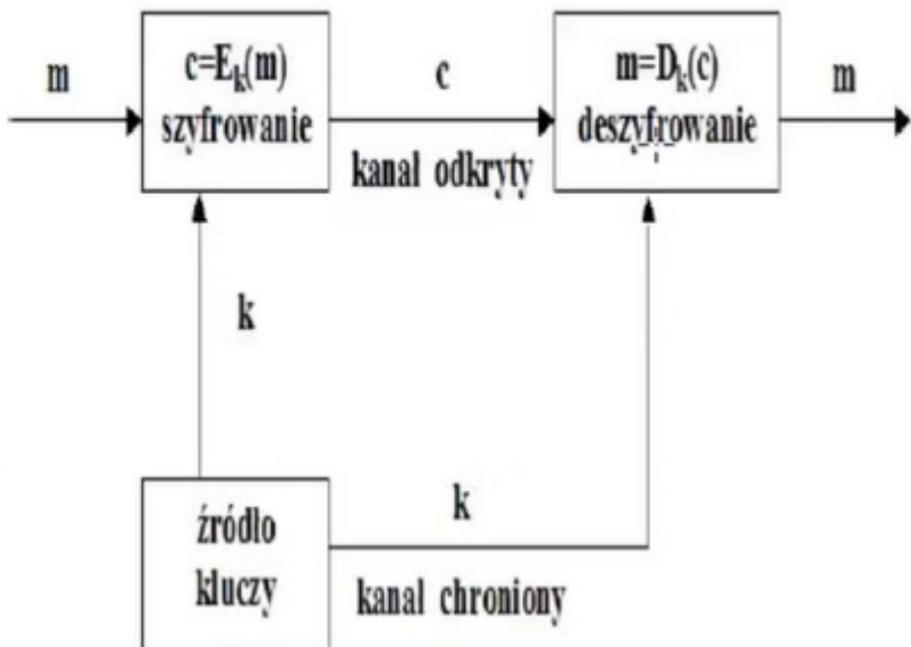
Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie



Szyfry współczesne

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykłdu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Szyfrowanie asymetryczne (systemy z kluczem publicznym i prywatnym):

I

- występują 2 klucze – klucz publiczny (jawny) oraz klucz prywatny (tajny),
- klucz publiczny służy do szyfrowania informacji a klucz prywatny służy do deszyfrowania informacji,

Szyfry współczesne

Wstęp do kryptografii

Piotr Mroczkowski

Wprowadzenie do przedmiotu

Plan wykładu

Podstawowe pojęcia i terminy

Podstawy matematyczne

Szyfry - charakterystyka

Podsumowanie

Szyfrowanie asymetryczne (systemy z kluczem publicznym i prywatnym):

- do wyznaczenia kluczy wykorzystuje się trudne do odwrócenia problemy, np.:
 - problem RSA (problem faktoryzacji liczb złożonych) - o wiele łatwiej jest pomnożyć przez siebie 2 duże liczby, niż rozłożyć dużą liczbę na czynniki pierwsze,
 - problem ElGamala - opierający się na trudności wyznaczania logarytmu dyskretnego.

Rodzaje bezpieczeństwa

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

Bezpieczeństwo obliczeniowe

kryptosystem jest obliczeniowo bezpieczny, jeśli moc obliczeniowa (zasoby pamięci, czas obliczeń) jest niewystarczająca do złamania tego kryptosystemu przy zastosowaniu najlepszych aktualnie metod kryptoanalizy.

Bezpieczeństwo bezwarunkowe

nie można złamać kryptosystemu niezależnie od posiadanych mocy obliczeniowych (np. szyfr Vernama).

Bezpieczeństwo warunkowe

atakujący dysponuje ograniczoną mocą obliczeniową, bezpieczeństwo szyfru oparte jest na aktualnej wiedzy i stanie technologii.

Szyfr Vernama (1917 r.)

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

Niech:

$p = p_1, p_2, \dots, p_n$, $p_i = \{0, 1\}$, $i = 1, 2, \dots, n$ - tekst jawnny,

$k = k_1, k_2, \dots, k_m$, $k_i = \{0, 1\}$, $i = 1, 2, \dots, m$ - klucz,

$c = c_1, c_2, \dots, c_n$, $c_i = \{0, 1\}$, $i = 1, 2, \dots, n$ - tekst zaszyfrowany,

Szyfr Vernama

szyfr, którego ciąg bitów tekstu zaszyfrowanego jest funkcją xor ciągu bitów tekstu jawnego i klucza:

- szyfrowanie: $c_i = p_i \oplus k_i$;
- deszyfrowanie: $p_i = c_i \oplus k_i$;

Dowód: $p_i = c_i \oplus k_i = p_i \oplus k_i \oplus k_i = p_i$.

Szyfr bezarunkowo bezpieczny

Szyfr Vernama, w którym ciąg klucza jest wybrany losowo i został użyty jednokrotnie nazywamy systemem z losowym kluczem jednorazowym (*one time pad*).

Techniki ataków

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

- Przeszukiwanie przestrzeni klucza (atak brutalny) – podatne na ten atak są wszystkie algorytmy oprócz szyfrów "one time pad".
- Metody oparte na analizie językowej, np. analiza częstości występowania liter.
- Ataki wykorzystujące budowę algorytmów.
- Kryptoanaliza liniowa.
- Kryptoanaliza różnicowa.
- Kryptoanaliza algebraiczna.
- Atak na implementację algorytmów (side channel attack).

Rodzaje bezpieczeństwa

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannon'a

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affinejny

Szyfr Vigenere'a

Szyfr Hilla

Bezpieczeństwo obliczeniowe

kryptosystem jest obliczeniowo bezpieczny, jeśli moc obliczeniowa (zasoby pamięci, czas obliczeń) jest niewystarczająca do złamania tego kryptosystemu przy zastosowaniu najlepszych aktualnie metod kryptoanalizy.

Bezpieczeństwo bezwarunkowe

nie można złamać kryptosystemu niezależnie od posiadanych mocy obliczeniowych (np. szyfr Vernama).

Bezpieczeństwo warunkowe

atakujący dysponuje ograniczoną mocą obliczeniową, bezpieczeństwo szyfru oparte jest na aktualnej wiedzy i stanie technologii.

Techniki ataków

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

- Przeszukiwanie przestrzeni klucza (atak brutalny) – podatne na ten atak są wszystkie algorytmy oprócz szyfrów "*one time pad*".
- Metody oparte na analizie językowej, np. analiza częstości występowania liter.
- Ataki wykorzystujące budowę algorytmów.
- Kryptoanaliza liniowa.
- Kryptoanaliza różnicowa.
- Kryptoanaliza algebraiczna.
- Atak na implementację algorytmów (side channel attack).

Analiza częstości występowania liter

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

- Każdy język naturalny ma nadmiarowość (redundancję) – w naturalnych tekstach poszczególne znaki alfabetu występują z określonymi częstotliwościami.
- Analizując typowe teksty możemy sporządzić tabele względnych częstości (prawdopodobieństw) występowania poszczególnych znaków.



Kodowanie alfabetu

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

Kodowanie alfabetu:

- każdej literze alfabetu przyporządkowujemy liczbę od 0 do 25:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
O	P	Q	R	S	T	U	V	W	X	Y	Z		
14	15	16	17	18	19	20	21	22	23	24	25		



Szyfr przesuwający - definicja

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannon'a

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony algorytm Euklidesa

Szyfr alfiniczny

Szyfr Vigenere'a

Szyfr Hilla

$P = \mathbb{Z}_{26}$ - skończony zbiór tekstów jawnych;

$C = \mathbb{Z}_{26}$ - skończony zbiór tekstów zaszyfrowanych;

$K = \mathbb{Z}_{26} - \{0\}$ - skończony zbiór kluczy;

■ szyfrowanie: $y = e_k(x) = (x + k) \bmod 26$;

■ deszyfrowanie: $x = d_k(y) = (y - k) \bmod 26$;

dla: $x \in P$, $y \in C$, dla $k \in K$.



Tabela częstości występowania liter (j. angielski)

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

Litera	Częstość	litera	Częstość
a	.082	n	.067
b	.015	o	.075
c	.028	p	.019
d	.043	q	.001
e	.127	r	.060
f	.022	s	.063
g	.020	t	.091
h	.061	u	.028
i	.070	v	.010
j	.002	w	.023
k	.008	x	.001
l	.040	y	.020
m	.024	z	.001

Podział liter vs. p-sto występowania (j. angielski)

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniiczny

Szyfr Vigenere'a

Szyfr Hilla

grupa	p-sto występowania	litery
1	$\geq 0,120$	e
2	$I(0,120 \dots 0,07]$	t,a,o,i
3	$(0,07 \dots 0,06]$	n,s,h,r
4	$(0,06 \dots 0,04]$	d,l
5	$(0,04 \dots 0,02]$	c,u,m,w,f,g
6	$\leq 0,02$	y,p,b,v,k,s,x,q

Analiza częstości występowania liter

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

- Sporządzamy tabele występowania znaków w szyfrogramie (dla nieznanego, ale ustalonego podstawienia).
- Na tej podstawie stawiamy hipotezę jak wygląda nieznane nam podstawienie i deszyfrujemy.
- Jeżeli otrzymamy tekst jawny to postawiona hipoteza jest prawdziwa, w prz. stawiamy kolejną hipotezę.
- Przy posiadaniu odpowiednio długiego szyfrogramu i wykonaniu prób przy różnych podstawieniach, metoda ta pozwala złamać prosty szyfr podstawieniowy.

Kodowanie alfabetu

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

Kodowanie alfabetu:

- każdej literze alfabetu przyporządkowujemy liczbę od 0 do 25:

A	B	C	D	E	F	G	H	I	J	K	L	M	N
0	1	2	3	4	5	6	7	8	9	10	11	12	13
O	P	Q	R	S	T	U	V	W	X	Y	Z		
14	15	16	17	18	19	20	21	22	23	24	25		



Szyfr przesuwający - kryptoanaliza

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

Kryptosystem oparty na szyfrze przesuwającym nie jest bezpieczny:

- Atak brytalny - wystarczy sprawdzić kolejno 25 wartości klucza $k \in \{1, 2, \dots, 25\}$ (średnio 13 prób).
- Analiza częstości występowania liter.

Przykład: Znajdź klucz oraz tekst jawny wiedząc, że tekst zaszyfrowany:

"FQLTWNYMRXFWJVZNYJLJSJWFQIJKN
SNYNTSXTKFWNYMRJYNHUWTHJXX"

lit.	il.												
N	7	Y	5	X	4	K	2	Q	2	U	1		
J	7	F	4	S	3	L	2	R	2	V	1		
W	5	T	4	H	2	M	2	I	1	Z	1		

Tabela częstości występowania liter (j. angielski)

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afimiczny

Szyfr Vigenere'a

Szyfr Hilla

Litera	Częstość	litera	Częstość
a	.082	n	.067
b	.015	o	.075
c	.028	p	.019
d	.043	q	.001
e	.127	r	.060
f	.022	s	.063
g	.020	t	.091
h	.061	u	.028
i	.070	v	.010
j	.002	w	.023
k	.008	x	.001
l	.040	y	.020
m	.024	z	.001

Szyfr przesuwający - kryptoanaliza

Wstęp do kryptologii

Piotr Mruczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiničny

Szyfr Vigenere'a

Szyfr Hilla

- 1 Zakładamy, że: $e \rightarrow N$, czyli:

$$y = e_k(x) = (x + k) \text{ mod } 26;$$

$$e_k(4) = 13;$$

$$4 + k = 13 \Rightarrow k = 9;$$

tekst jawny:

"whcknepdiownnamqepacajanwhzabejepekjokbwnepeylnkyao"

- 2 Zakładamy, że: $e \rightarrow J$, czyli:

$$e_k(4) = 9;$$

$$4 + k = 9 \Rightarrow k = 5;$$

tekst jawny:

"algorithms are quite general definitions of arithmetic process"

algorithms are quite general definitions of arithmetic process

Algorytm Euklidesa, 300 r.p.n.e.

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiničny

Szyfr Vigenere'a

Szyfr Hilla

I

Dane wejściowe: dwie nieujemne liczby całkowite $a, b \in \mathbb{Z}^+$, $a \geq b$.

Dane wyjściowe: największy wspólny dzielnik: $d = \gcd(a, b)$.

1 Jeśli $b = 0$ to $d \leftarrow a$, zwróć d ;

2 Podziel a przez b otrzymując:

- cześć całkowitą dzielenia: $q = a \text{ div } b$;
- resztę dzielenia: $r = a \text{ mod } b$

takie, że $a = q \cdot b + r$.

3 Jeśli $r = 0$ to $d \leftarrow b$, zwróć d ,

w p.p. podstaw $a \leftarrow b$, $b \leftarrow r$ i idź do pkt. 2;

Rozszerzony Algorytm Euklidesa

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniyczny

Szyfr Vigenere'a

Szyfr Hilla

Dane wejściowe: dwie nieujemne liczby całkowite $a, b \in \mathbb{Z}^+$, $a \geq b$.
Dane wyjściowe: (d, u, v) , gdzie: $d = \gcd(a, b)$, u i v - liczby spełniające warunek: $u \cdot a + v \cdot b = \gcd(a, b)$.

- 1 Jeśli $b = 0$ to $d \leftarrow a$, zwróć $(d, 1, 0)$, stop.
- 2 Podstaw: $i \leftarrow 0$, $(u_0, v_0) \leftarrow (0, 1)$, $(u'_0, v'_0) \leftarrow (1, 0)$,
 $a_0 \leftarrow a$, $b_0 \leftarrow b$.
- 3 Oblicz: $q_i = a_i \text{ div } b_i$, $r_i = a_i \text{ mod } b_i$.
- 4 Jeśli $r_i = 0$ to $d \leftarrow b_i$, zwróć (d, u_i, v_i) , stop.
- 5 Podstaw: $i \leftarrow i + 1$,
 $u_i \leftarrow u'_{i-1} - q_{i-1} \cdot u_{i-1}$, $u'_i \leftarrow u_{i-1}$,
 $v_i \leftarrow v'_{i-1} - q_{i-1} \cdot v_{i-1}$, $v'_i \leftarrow v_{i-1}$,
 $a_i \leftarrow b_{i-1}$, $b_i \leftarrow r_{i-1}$,
- 6 Wróć do kroku 3.

Odwrotność multiplikatywna $a^{-1} \bmod n$

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannon'a

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony algorytm Euklidesa

Szyfr afiničny

Szyfr Vigenere'a

Szyfr Hilla

Definicja

Odwrotnością multiplikatywną $a \in Z_n$ modulo n nazywamy liczbę całkowitą $a^{-1} \in Z_n$ taką, że $a \cdot a^{-1} \equiv 1 \bmod n$.



Obliczanie $a^{-1} \bmod n$ z tw. Fermata

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

Twierdzenie Fermata

Jeśli p jest liczbą pierwszą, to dla każdej liczby $a \in \mathbb{Z}$ takiej, że $\gcd(a, p) = 1$ zachodzi:

$$a^{p-1} \bmod p = 1$$

Uogólnienie Eulera twierdzenia Fermata

Dla każdego $a \in \mathbb{Z}$ i $n \in \mathbb{N}$ takich, że $\gcd(a, n) = 1$ zachodzi:

$$a^{\phi(n)} \bmod n = 1$$

□

$$a^{\phi(n)} \cdot a^{-1} \bmod n = a^{-1};$$

$$a^{-1} = a^{(\phi(n)-1)} \bmod n.$$

Obliczanie $a^{-1} \bmod n$ z tw. Fermata

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

Przykład: Oblicz odwrotność multiplikatywną liczby $a = 11 \bmod 125$ korzystając z uogólnionego twierdzenia Fermata.

Twierdzenie

Jeśli $n = p_1^{e_1} \cdots p_k^{e_k}$ jest rozkładem na czynniki pierwsze, to:

$$\phi(n) = \prod_{i=1}^k p_i^{e_i-1} \cdot (p_i - 1)$$

$$n = 125 = 5^3;$$

$$\phi(n) = 5^2 \cdot 4 = 25 \cdot 4 = 100;$$

$$a^{-1} = a^{(\phi(n)-1)} \bmod n = 11^{100-1} \bmod 125 = 11^{99} \bmod 125 = 91.$$

Szyfr afiniczny - definicja

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniczny

Szyfr Vigenere'a

Szyfr Hilla

$P = \mathbb{Z}_{26}$ - skończony zbiór tekstów jawnych;

$C = \mathbb{Z}_{26}$ - skończony zbiór tekstów zaszyfrowanych;

$K = \{(a, b) : a \in \mathbb{Z}_{26}^*, b \in \mathbb{Z}_{26}\}$ - skończony zbiór kluczy;

- szyfrowanie przy użyciu klucza $k = (a, b) \in K$:

$$y = e_k(x) = (a \cdot x + b) \bmod 26$$

- deszyfrowanie przy użyciu klucza

$$k' = (a', b') = (a^{-1}, -a^{-1} \cdot b) \in K:$$

$$x = d_{k'}(y) = (a' \cdot y + b') \bmod 26 = (a^{-1} \cdot y + (-a^{-1} \cdot b)) \bmod 26$$

gdzie: $x \in P$, $y \in C$,

I

$\mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$ - zbiór liczb całkowitych modulo 26;

$\mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ - zbiór liczb odwracalnych w \mathbb{Z}_{26} ;

Szyfr afiniczny - kryptoanaliza

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannon'a

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniczny

Szyfr Vigenere'a

Szyfr Hilla

1 Zakładamy, że: $e \rightarrow R$ i $t \rightarrow K$ czyli:

$$e_k(4) = 17 \text{ i } e_k(19) = 7;$$

i otrzymujemy układ równań:

$$4a + b = 17$$

$$19a + b = 10,$$

który daje rozwiązanie: $a = 3$, $b = 5$ w Z_{26} , czyli

$$k = (3, 5), k' = (9, 7).$$

tekst jawnny:

"algorithmsarequitегeneraldefinitionsofarithmeticprocess"

Szyfr afiniczny - własności

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniczny

Szyfr Vigenere'a

Szyfr Hilla

Własności szyfru przesuwającego:

- 1 szyfr afiniczny dla $a = 1$ jest szyfrem przesuwającym z kluczem b ;
- 2 jest szyfrem monoalfabetycznym;
- 3 przestrzeń klucza: $12 \cdot 26 = 312$.

I

Szyfr afiniaczny - kryptoanaliza

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniaczny

Szyfr Vigenere'a

Szyfr Hilla

Kryptosystem oparty na szyfrze afiniaczny nie jest bezpieczny:

- Atak brytalny - wystarczy sprawdzić kolejno 312 wartości klucza k (średnio 156 prób).
- Analiza częstości występowania liter.

Przykład: Znajdź klucz oraz tekst jawny wiedząc, że tekst zaszyfrowany:

"FMXVEDKAPHFERBNDKRXRSREFMORU
DSDKDVSHVUFEDKAPRKDLYEVLRHH"

lit.	il.												
D	7	K	5	V	4	L	2	U	2	N	1		
R	7	F	4	S	3	M	2	X	2	O	1		
E	5	H	4	A	2	P	2	B	1	Y	1		

Szyfr afiniczny - kryptoanaliza

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniczny

Szyfr Vigenere'a

Szyfr Hilla

I Zakładamy, że: $e \rightarrow R$ i $t \rightarrow D$ czyli:

$$e_k(4) = 17 \text{ i } e_k(19) = 3;$$

i otrzymujemy układ równań:

$$4a + b = 17$$

$$19a + b = 3,$$

który daje rozwiązanie: $a = 6$, $b = 19$ w Z_{26} .

Ponieważ $\gcd(6, 26) = 2 \neq 1$ to rozwiązanie jest błędne.

Podział liter vs. p-sto występowania (j. angielski)

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

grupa	p-sto występowania	litery
1	$\geq 0,120$	£
2	(0,120 ... 0,07]	t,a,o,i
3	(0,07 ... 0,06]	n,s,h,r
4	(0,06 ... 0,04]	d,l
5	(0,04 ... 0,02]	c,u,m,w,f,g
6	$\leq 0,02$	y,p,b,v,k,s,x,q

Szyfr afiniczny - kryptoanaliza

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Sharmona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniczny

Szyfr Vigenere'a

Szyfr Hilla

1 Zakładamy, że: $\mathbb{Z} \rightarrow R$ i $t \rightarrow D$ czyli:

$$e_k(4) = 17 \text{ i } e_k(19) = 3;$$

i otrzymujemy układ równań:

$$4a + b = 17$$

$$19a + b = 3,$$

który daje rozwiązanie: $a = 6, b = 19$ w Z_{26} .

Ponieważ $gcd(6, 26) = 2 \neq 1$ to rozwiązanie jest błędne.

Szyfr afiniczny - definicja

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniczny

Szyfr Vigenere'a

Szyfr Hilla

$P = \mathbb{Z}_{26}$ - skończony zbiór tekstów jawnych;

$C = \mathbb{Z}_{26}$ - skończony zbiór tekstów zaszyfrowanych;

$K = \{(a, b) : a \in \mathbb{Z}_{26}^*, b \in \mathbb{Z}_{26}\}$ - skończony zbiór kluczy;

- szyfrowanie przy użyciu klucza $k = (a, b) \in K$:

$$y = e_k(x) = (a \cdot x + b) \bmod 26$$

- deszyfrowanie przy użyciu klucza

$$k' = (a', b') = (a^{-1}, -a^{-1} \cdot b) \in K:$$

$$x = d_{k'}(y) = (a' \cdot y + b') \bmod 26 = (a^{-1} \cdot y + (-a^{-1} \cdot b)) \bmod 26$$

gdzie: $x \in P$, $y \in C$,

$\mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$ - zbiór liczb całkowitych modulo 26;

$\mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ - zbiór liczb odwracalnych w \mathbb{Z}_{26} ;

Szyfr afiniczny - przykład

Wstęp do kryptologii

Piotr

Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniczny

Szyfr Vigenere'a

Szyfr Hilla

Przykład: Zaszyfruj, a następnie zdeszyfruj "kryptografia" przy użyciu klucza $k = (5, 10)$.

■ Szyfrowanie

PT	k	r	p	p	t	o	g	r	s	l	i	s
x	10	17	24	15	19	14	6	17	0	5	8	0
y	8	17	0	7	1	2	14	17	10	9	24	10
CT	I	R	A	H	B	C	O	R	K	J	Y	K

Tekst zaszyfrowany: IRAHBCORKJYK.

■ Deszyfrowanie

$$n = 26 = 2 \cdot 13$$

$$\phi(n) = \prod_{i=1}^k p_i^{e_i-1} \cdot (p_i - 1) = 2^0 \cdot 1 \cdot 13^0 \cdot 12 = 1 \cdot 12 = 12$$

$$a^{-1} = a^{(\phi(n)-1)} \bmod n = 5^{11} \bmod 26 = 21$$

$$k' = (a^{-1}, -a^{-1} \cdot b) = (21, (-21 \cdot 10) \bmod n) = (21, 24)$$

CT	I	R	A	H	B	C	O	R	K	J	Y	K
y	8	17	0	7	1	2	14	17	10	9	24	10
x	10	17	24	15	19	14	6	17	0	5	8	0
PT	k	r	y	p	t	o	g	r	s	l	i	s

Tekst jawny : kryptografia.

Szyfr afiniczny - kryptoanaliza

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniczny

Szyfr Vigenere'a

Szyfr Hilla

Kryptosystem oparty na szyfrze afincznym nie jest bezpieczny:

- Atak brytalny - wystarczy sprawdzić kolejno 312 wartości klucza k (średnio 156 prób).
- Analiza częstości występowania liter.

Przykład: Znajdź klucz oraz tekst jawny wiedząc, że tekst zaszyfrowany:

"FMXVEDKAPHFERBNDKRXRSREFMORU
DSDKDVSHVUFEDKAPRKDLYEVLRHH"

lit.	il.	il.										
D	7	K	5	V	4	L	2	U	2	N	1	
R	7	F	4	S	3	M	2	X	2	O	1	
E	5	H	4	A	2	P	2	B	1	Y	1	

Szyfr afiniczny - kryptoanaliza

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniczny

Szyfr Vigenere'a

Szyfr Hilla

- 1 Zakładamy, że: $e \rightarrow R$ i $t \rightarrow D$ czyli:

$$e_k(4) = 17 \text{ i } e_k(19) = 3;$$

i otrzymujemy układ równań:

$$4a + b = 17$$

$$19a + b = 3,$$

który daje rozwiązanie: $a = 6, b = 19$ w Z_{26} .

Ponieważ $\gcd(6, 26) = 2 \neq 1$ to rozwiązanie jest błędne.

- 2 Zakładamy, że: $e \rightarrow R$ i $t \rightarrow E$ czyli:

$$e_k(4) = 17 \text{ i } e_k(19) = 4;$$

i otrzymujemy układ równań:

$$4a + b = 17$$

$$19a + b = 4,$$

który daje rozwiązanie: $a = 13, b = 17$ w Z_{26} . Ponieważ

$\gcd(13, 26) = 13 \neq 1$ to rozwiązanie jest błędne.

Szyfr afiniaczny - definicja

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

$P = \mathbb{Z}_{26}$ - skończony zbiór tekstów jawnych;

$C = \mathbb{Z}_{26}$ - skończony zbiór tekstów zaszyfrowanych;

$K = \{(a, b) : a \in \mathbb{Z}_{26}^*, b \in \mathbb{Z}_{26}\}$ - skończony zbiór kluczy;

- szyfrowanie przy użyciu klucza $k = (a, b) \in K$:

$$y = e_k(x) = (a \cdot x + b) \bmod 26$$

- deszyfrowanie przy użyciu klucza

$$k' = (a', b') = (a^{-1}, -a^{-1} \cdot b) \in K:$$

$$x = d_{k'}(y) = (a' \cdot y + b') \bmod 26 = (a^{-1} \cdot y + (-a^{-1} \cdot b)) \bmod 26$$

gdzie: $x \in P$, $y \in C$,

$\mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$ - zbiór liczb całkowitych modulo 26;

$\mathbb{Z}_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$ - zbiór liczb odwracalnych w \mathbb{Z}_{26} ;

Szyfr afiniczny - kryptoanaliza

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony algorytm Euklidesa

Szyfr afiniczny

Szyfr Vigenere'a

Szyfr Hilla

1 Zakładamy, że: $e \rightarrow R$ i $t \rightarrow K$ czyli:

$$e_k(4) = 17 \text{ i } e_k(19) = 7;$$

i otrzymujemy układ równań:

$$4a + b = 17$$

$$19a + b = 10,$$

który daje rozwiązanie: $a = 3$, $b = 5$ w Z_{26} , czyli
 $k = (3, 5)$, $k' = (9, 7)$.

tekst jawnny:

"algorithmsarequitegeneraldefinitionsofarithmeticprocess"



Szyfr Vigenere'a - definicja

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

$P = (\mathbb{Z}_{26})^m$ - skończony zbiór tekstów jawnych;

$C = (\mathbb{Z}_{26})^m$ - skończony zbiór tekstów zaszyfrowanych;

$K = (\mathbb{Z}_{26})^m$ - skończony zbiór kluczy;

■ szyfrowanie:

$$y = e_k(x_1, \dots, x_m) = ((x_1 + k_1) \bmod 26, \dots, (x_m + k_m) \bmod 26);$$

■ deszyfrowanie:

$$x = d_k(y_1, \dots, y_m) = \begin{matrix} I \\ ((y_1 - k_1) \bmod 26, \dots, (y_m - k_m) \bmod 26); \end{matrix}$$

gdzie: $x = (x_1, \dots, x_m) \in P$, $y = (y_1, \dots, y_m) \in C$,
 $k = (k_1, \dots, k_m) \in K$.

Szyfr Vigenere'a - przykład

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannon'a

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiniiczny

Szyfr Vigenere'a

Szyfr Hilla

Przykład: Zaszyfruj a potem odszyfruj słowo "kryptografia" przy użyciu klucza "szyfr".
I

$$m = 5, \quad k = \text{"szyfr"} = (18, 25, 24, 5, 17)$$

PT	k	i	y	p	t	o	a	r	s	f	i	a
x	10	17	24	15	19	14	6	17	0	5	8	0
k	18	25	24	5	17	10	25	24	5	17	18	25
y	2	18	22	20	10	6	5	15	5	22	0	25
CT	C	Q	W	U	K	G	F	P	F	W	A	Z

tekst zaszyfrowany: CQWUKGFPFWAZ

Szyfr Vigenere'a - własności

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr afiński

Szyfr Vigenere'a

Szyfr Hilla

Własności szyfru przesuwającego:

- jest szyfrem polialfabetycznym;
- przestrzeń klucza: $\#K = 26^m$ (np. dla $m = 5$ przestrzeń klucza większa niż $1,1 \cdot 10^7$); I
- jeśli klucz ma długość tekstu jawnego (np. jest innym tekstem z danego języka) nazywany jest **szyfrem z kluczem bieżącym**;
- jeśli dodatkowo klucz jest losowym ciągiem liter oraz został użyty jednokrotnie jest bezwarunkowo bezpieczny i nazywany **szyfrem z kluczem jednokrotnym**;
- w przeciwnym przypadku istnieją metody kryptoanalizy pozwalające złamać szyfr Vigenere'a w czasie krótszym niż przeszukiwanie przestrzeni klucza.

Szyfr Vigenere'a - przykład

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannon'a

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

Przykład: Zaszyfruj a potem odszyfruj słowo "kryptografia" przy użyciu klucza "szyfr".

$$m = 5, \quad k = \text{"szyfr"} = (18, 25, 24, 5, 17)$$

PT	k	t	y	p	t	o	a	r	a	t	i	a
x	10	17	24	15	19	14	6	17	0	5	8	0
k	18	25	24	5	17	10	25	24	5	17	18	25
y	2	16	22	20	10	6	5	15	5	22	0	25
CT	C	Q	W	U	K	G	F	P	F	W	A	Z

tekst zaszyfrowany: CQWUKGFPFWAZ

Szyfr Hilla, cz. 1

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannona

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

$P = (\mathbb{Z}_{26})^m$ - skończony zbiór tekstów jawnych;

$C = (\mathbb{Z}_{26})^m$ - skończony zbiór tekstów zaszyfrowanych;

$$K = \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix}$$

- macierz o wymiarze $m \times m$

■ szyfrowanie:

$$y = e_K(x) = (x \cdot K) \bmod 26;$$

■ deszyfrowanie:

$$x = e_{K^{-1}}(y) = (y \cdot K^{-1}) \bmod 26;$$

gdzie: $x = (x_1, x_2, \dots, x_m) \in P$, $y = (y_1, y_2, \dots, y_m) \in C$,

K^{-1} - macierz odwrotana modulo 26 do macierzy K , tzn:

$$\gcd(\det K, 26) = 1$$

Szyfr Hilla, cz. 2

Wstęp do kryptologii

Piotr Mroczkowski

Plan wykładu

Twierdzenie Shannon'a

Rodzaje bezpieczeństwa

Kodowanie alfabetu

Szyfr przesuwający

Rozszerzony Algorytm Euklidesa

Szyfr affineczny

Szyfr Vigenere'a

Szyfr Hilla

■ szyfrowanie:

$$y = (x_1, x_2, \dots, x_m) \cdot \begin{bmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{bmatrix} \text{ mod } 26;$$

■ deszyfrowanie:

$$x = (y_1, y_2, \dots, y_m) \cdot \begin{bmatrix} k_{11}^{-1} & k_{12}^{-1} & \dots & k_{1m}^{-1} \\ k_{21}^{-1} & k_{22}^{-1} & \dots & k_{2m}^{-1} \\ \dots & \dots & \dots & \dots \\ k_{m1}^{-1} & k_{m2}^{-1} & \dots & k_{mm}^{-1} \end{bmatrix} \text{ mod } 26;$$

gdzie: $x = (x_1, x_2, \dots, x_m) \in P$, $y = (y_1, y_2, \dots, y_m) \in C$.



Algorytm szybkiego potęgowania modularnego

Potęgowanie modularne

Potęgowanie modularne polega na obliczeniu:

$$x = a^t \bmod n$$

gdzie: $t, n \in N$, $a, x \in Z_n$

Algorytm szybkiego potęgowania modularnego

Niech $t = (t_{k-1}, \dots, t_1, t_0)_2$, gdzie $t_i \in \{0, 1\}$, $i = 0, 1, \dots, k-1$ będzie rozwinięciem dwójkowym liczby t :

$$\sum t_i \cdot 2^{i-1} = 2^{k-1} \cdot t_{k-1} + \dots + 2^1 \cdot t_1 + 2^0 \cdot t_0$$

Wówczas:

$$a^t \bmod n = [(a^{t_{k-1}2^{k-1}} \bmod n) \cdot \dots \cdot (a^{t_12^1} \bmod n) \cdot (a^{t_02^0} \bmod n)] \bmod n$$

Algorytm szybkiego potęgowania modularnego

Algorytm szybkiego potęgowania modularnego

- 1 Inicjalizacja: $i \leftarrow 0$, $x_0 \leftarrow 1$, $a_0 \leftarrow a$.
- 2 Wyznacz: $i \leftarrow i + 1$.
- 3 Jeśli $t_{i-1} = 1$ wtedy $x_i \leftarrow (x_{i-1} \cdot a_{i-1}) \bmod n$, w przeciwnym przypadku $x_i \leftarrow x_{i-1}$.
- 4 Jeśli $i = k$, zwróć x_k , stop.
- 5 Wyznacz $a_i \leftarrow (a_{i-1} \cdot a_{i-1}) \bmod n$ i idź do pkt. 2.

Przykład: Oblicz $2^{25} \bmod 9 = 2$.
 $a = 2$; $t = 25 = (11001)_2$; $n = 9$

i	x_i	a_i	t_i
0	1	2	1
1	2	4	0
2	2	7	0
3	2	4	1
4	8	7	1
5	2	4	-

**WSTĘP DO
KRYPTOLOGII**

dr inż. Piotr
Mroczkowski

Wyznacznik

Kryptografia
klucza publicznego
i asymetryczna

Generator grupy
mendolityzowej

Lagrange
dzielenie

Protokół
Diffie-Hellman'a

Idea
kryptografii
asymetrycznych

Kryptografia asymetryczna Kryptografia klucza publicznego



dr inż. Piotr Mroczkowski

Plan wykładu

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modularnego

Generator grupy mnożnikowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

- 1 Algorytm szybkiego potęgowania modularnego.
- 2 Generator grupy mnożnikowej.
- 3 Logarytm dyskretny.
- 4 Algorytm Diffie-Hellman'a.
- 5 Idea kryptosystemów asymetrycznych

Algorytm szybkiego potęgowania modularnego

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Algorytm
szybkiego
potęgowania
modularnego

Generator grupy
mobilipatytwnej

Logarytm
dyskretny

Protokół
Diffie-Hellman'a

Idea
kryptosystemów
asymetrycznych

Potęgowanie modularne

Potęgowanie modularne polega na obliczeniu:

$$x = a^t \bmod n$$

gdzie: $t, n \in \mathbb{N}$, $a, x \in \mathbb{Z}_n$

Algorytm szybkiego potęgowania modularnego

Niech $t = (t_{k-1}, \dots, t_1, t_0)_2$, gdzie $t_i = \{0, 1\}$, $i = 0, 1, \dots, k-1$
będzie rozwinięciem dwójkowym liczby t :

$$t = 2^{k-1} \cdot t_{k-1} + \dots + 2^1 \cdot t_1 + 2^0 \cdot t_0$$

Wówczas:

$$a^t \bmod n = [(a^{t_{k-1}2^{k-1}} \bmod n) \cdot \dots \cdot (a^{t_12^1} \bmod n) \cdot (a^{t_02^0} \bmod n)] \bmod n$$

Algorytm szybkiego potęgowania modularnego

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Algorytm
szybkiego
potęgowania
modularnego

Generator grupy
mulektywnej

Logarytm
dyskretny

Protokół
Diffie-Hellmana

Idea
kryptosystemów
asymetrycznych

Algorytm szybkiego potęgowania modularnego

- 1 Inicjalizacja: $i \leftarrow 0$, $x_0 \leftarrow 1$, $a_0 \leftarrow a$.
- 2 Wyznacz: $i \leftarrow i + 1$.
- 3 Jeżeli $t_{i-1} = 1$ wtedy $x_i \leftarrow (x_{i-1} \cdot a_{i-1}) \bmod n$, w przeciwnym
przypadku $x_i \leftarrow x_{i-1}$.
- 4 Jeżeli $i = k$, zwróć x_i , stop.
- 5 Wyznacz $a_i \leftarrow (a_{i-1} \cdot a_{i-1}) \bmod n$ i idź do pkt. 2.

Przykład: Oblicz $2^{25} \bmod 9 = 2$.
 $a = 2$; $t = 25 = (11001)_2$; $n = 9$

i	x_i	a_i	t_i
0	1	2	1
1	2	4	0
2	2	7	0
3	2	4	1
4	8	7	1
5	2	4	-

Generator grupy mnożkowej

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Algorytm
szybkiego
potęgowania
modularnego

Generator grupy
mnożkowej

Logarytm
dyskretny

Protokół
Diffie-Hellman'a

Idea
kryptosystemów
asymetrycznych

Niech $Z_p^* = \{x : x \in Z_p, \gcd(x, p) = 1\}$ będzie zbiorem elementów odwracalnych modulo liczba pierwsza p .

Generator

Liczbe $\alpha \in Z_p^*$ nazywamy **generatorem Z_p^* (pierwiastkiem pierwotnym modulo p)** wtedy i tylko wtedy gdy:

$$\bigwedge_{y \in Z_p^*} \bigvee_{x \in Z_p^*} y = \alpha^x \bmod p$$

Można więc powiedzieć, że α jest generatorem Z_p^* , jeśli kolejne potęgi α modulo p generują wszystkie elementy zbioru Z_p^* .

▀

Generator grupy mnożkowej

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modułarnego

Generator grupy mnożkowej

Logarytm dyskretny

Protokół Diffie-Hellmana

Idea kryptosystemów asymetrycznych

Niech $p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}$ będzie rozkładem liczby $p - 1$ na czynniki pierwsze.

I

Twierdzenie

α jest generatorem Z_p^* $\Leftrightarrow \bigwedge_{i \in \{1, 2, \dots, k\}} \alpha^{\frac{p-1}{p_i}} \bmod p \neq 1$

Generator grupy mnożkowej

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modularnego

Generator grupy mnożkowej

Lagarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

Przykład:

Sprawdź, czy $\alpha = 2$ jest generatorem Z_7^* .

$$p - 1 = 6 = 2 \cdot 3; p_1 = 2, p_2 = 3.$$

i	p_i	$\alpha^{\frac{p-1}{p_i}} \bmod p$	wynik
1	2	$2^{\frac{6}{2}} \bmod 7 = 2^3 \bmod 7 = 1$	F

Przykład:

Sprawdź, czy $\alpha = 3$ jest generatorem Z_7^* .

$$p - 1 = 6 = 2 \cdot 3; p_1 = 2, p_2 = 3.$$

i	p_i	$\alpha^{\frac{p-1}{p_i}} \bmod p$	wynik
1	2	$3^{\frac{6}{2}} \bmod 7 = 3^3 \bmod 7 = 6 \neq 1$	T
2	3	$3^{\frac{6}{3}} \bmod 7 = 3^2 \bmod 7 = 2 \neq 1$	T

Logarytm dyskretny

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Algorytm
szybkiego
potęgowania
modularnego

Generator grupy
mnożenia

Algorytm
dyskretny

Protokół
Diffie-Hellman'a

Idea
kryptosystemów
asymetrycznych

Niech $Z_p^* = \{x : x \in Z_p, \gcd(x, p) = 1\}$ będzie zbiorem elementów odwracalnych modulo liczba pierwsza p .

Niech α będzie generatorem Z_p^* oraz $\beta \in Z_p^*$.

Definicja logarytmu dyskretnego

Logarytmem dyskretnym z β przy podstawie α , oznaczanym $\log_{\alpha}\beta$, jest unikatowa liczba całkowita $x \in Z_p^*$, taka że $\beta = \alpha^x \bmod p$.

Przykład:

Niech $\alpha = 5$ będzie generatorem Z_{97}^* oraz $\beta = 35$.

Logarytm dyskretny $\log_5 35 = 32$, ponieważ $35 = 5^{32} \bmod 97$.

Problem logarytmu dyskretnego

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Algorytm
szybkiego
potęgowania
modularnego

Generator grupy
mobilipatywnej

Logarytm
dyskretny

Protokół
Diffie-Hellman'a

Idea
kryptosystemów
asymetrycznych

Niech p będzie liczbą pierwszą.

Problem logarytmu dyskretnego - DLP

Dla danego generatora α grupy Z_p^* oraz elementu $\beta \in Z_p^*$ znaleźć:

$$x = \log_{\alpha} \beta$$

takie, że $\beta = \alpha^x \bmod p$.

Przykład: Obliczyć $\log_5 18$ w Z_{23}^*

Znaleźć $x \in \{0, 1, \dots, 22\}$ takie, że $5^x \bmod 23 = 18$.

W tym celu obliczmy:

$$5^1 \bmod 23 = 5,$$

$$5^2 \bmod 23 = 2,$$

$$5^3 \bmod 23 = 10, \dots, 5^{12} \bmod 23 = 18$$

Stąd $x = 12$

Protokół Diffie-Hellman'a - New Directions in Cryptography, 1976

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modułarnego

Generator grupy mnożnikowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

Protokół uzgadniania kluczy Diffie-Hellman'a

protokół kryptograficzny, w wyniku wykonania którego dwie strony otrzymują taką samą liczbę, przy czym otrzymanie tej liczby na podstawie treści wymienionych wiadomości między stronami jest praktycznie niemożliwe. Liczba ta może być używana jako klucz do szyfrowania komunikacji.

- 1 Bezpieczeństwo oparte na trudności obliczania logarytmów dyskretnych w ciałach skończonych.
- 2 Wykorzystywany do dystrybucji kluczy (uzgadniania klucza).



Protokół Diffie-Hellman'a - New Directions in Cryptography, 1976

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modułarnego

Generator grupy mnożkowej

Lagarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

Protokół uzgadniania kluczy Diffie-Hellman'a

protokół kryptograficzny, w wyniku wykonania którego dwie strony otrzymują taką samą liczbę, przy czym otrzymanie tej liczby na podstawie treści wymienionych wiadomości między stronami jest praktycznie niemożliwe. Liczba ta może być używana jako klucz do szyfrowania komunikacji.

- 1 Bezpieczeństwo oparte na trudności obliczania lagarytmów dyskretnych w ciałach skończonych.
- 2 Wykorzystywany do dystrybucji kluczy (uzgadniania klucza).



Algorytm Diffie-Hellman'a

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modularnego

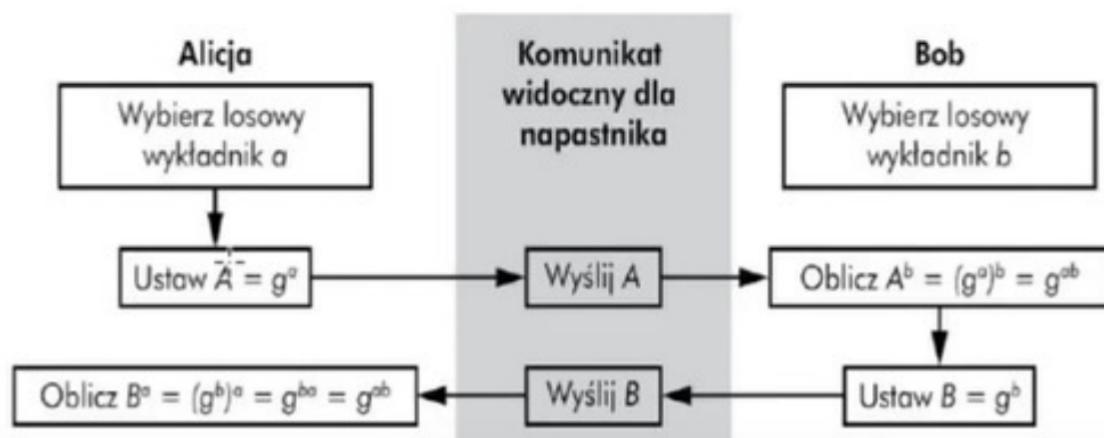
Generator grupy mnożkowej

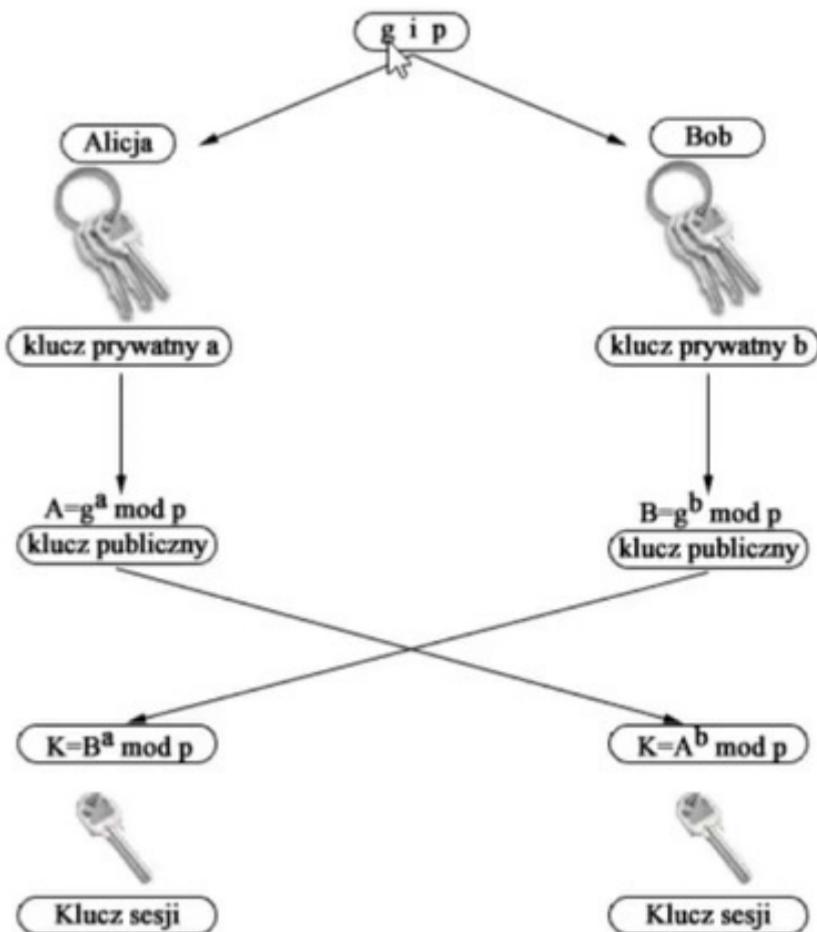
Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

- Alicja i Bob uzgadniają dużą liczbę pierwszą p oraz generator g grupy mnożkowej Z_p^* .
- Liczby te mogą być opublikowane wcześniej lub uzgodnione przez sieć.
- Ich tajność nie jest istotna dla bezpieczeństwa protokołu.





Algorytm Diffie-Hellman'a

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modułarnego

Generator grupy mnożkowej

Algorytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

- 1 Alicja wybiera losowo dużą liczbę całkowitą $1 < a < p - 1$ i oblicza:

$$A = g^a \text{ mod } p$$

- 2 Bob wybiera losowo dużą liczbę całkowitą $1 < b < p - 1$ i oblicza:

$$B = g^b \text{ mod } p$$

- 3 Alicja wysyła A do Boba, Bob wysyła B do Alicji

- 4 Alicja oblicza: $k_A = B^a \text{ mod } p$

- 5 Bob oblicza: $k_B = A^b \text{ mod } p$

$$k = k_A = k_B = g^{ab} \text{ mod } p$$

Atak Man-in-the-Middle na algorytm D-H

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

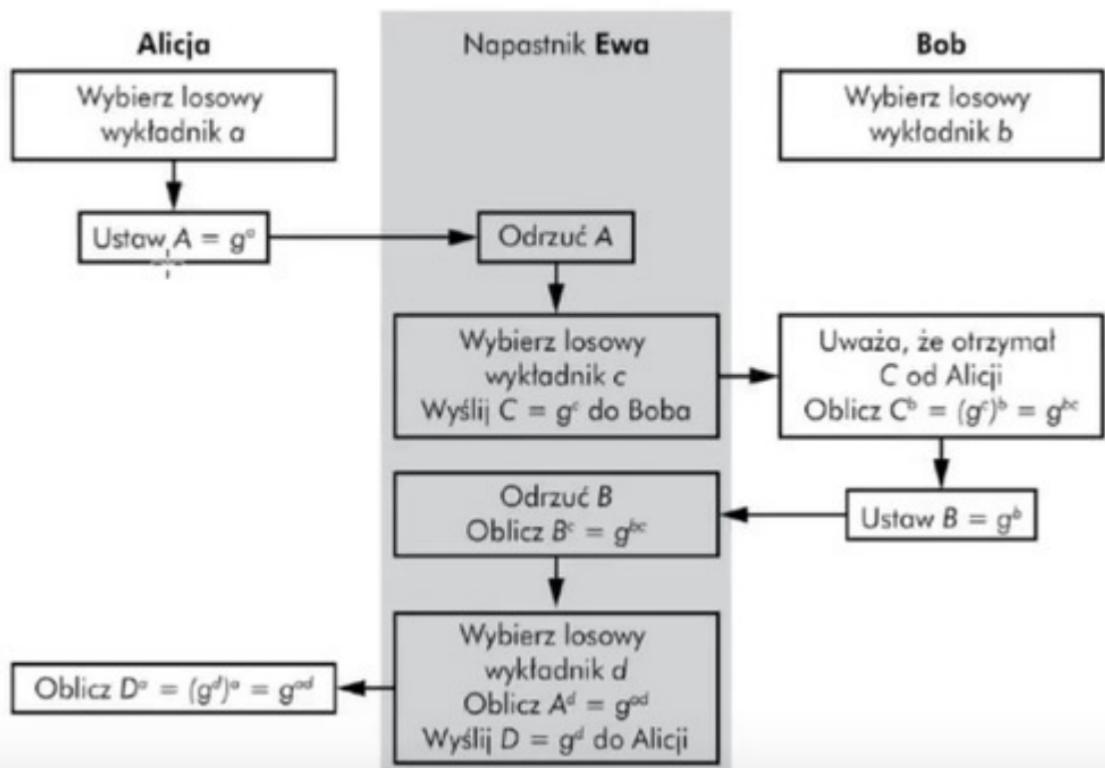
Algorytm szybkiego potęgowania modułarnego

Generator grupy mnożkowej

Algorytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych



Algorytm Diffie-Hellman'a - bezpieczeństwo, cz. 1

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modułarnego

Generator grupy mnożenia

Logarytm dyskretny

Protokół Diffie-Hellman'a

Identyfikacja kryptosystemów asymetrycznych

Problem Diffiego-Hellmana

Dla:

- danej liczby pierwszej p ,
- generatora g grupy \mathbb{Z}_p^* ,
- elementów $g^a \text{ mod } p$ oraz $g^b \text{ mod } p$,

znać liczbę całkowitą $g^{ab} \text{ mod } p$.

Algorytm Diffie-Hellman'a - bezpieczeństwo, cz. 2



WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potegowania modułarnego

Generator grupy mnożkowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

- Podsłuchujący zna tylko p , g , $A = g^a \text{ mod } p$, $B = g^b \text{ mod } p$.
- Aby znaleźć k musi wyznaczyć a i b obliczając logarytmy dyskretnie:

$$a = \log_g A$$

$$b = \log_g B$$

- Warunki bezpieczeństwa:
 - 1 p i $(p - 1)/2$ - liczby pierwsze długości min. 2048 bity ,
 - 2 g - pierwiastek pierwotny modulo p .

Rozszerzony algorytm Diffie-Hellman'a, cz. 1

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modularnego

Generator grupy mnożenia

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

Alicja, Bob i Karol ustalają:

- dużą liczbę pierwszą p taką, że liczba $(p - 1)/2$ też jest pierwszą,
- generator g grupy mnożenia Z_p^* .

- 1 Alicja wybiera losowo dużą liczbę całkowitą a i oblicza:

$$A = g^a \bmod p$$

- 2 Bob wybiera losowo dużą liczbę całkowitą b i oblicza:

$$B = g^b \bmod p$$

- 3 Karol wybiera losowo dużą liczbę całkowitą c i oblicza:

$$C = g^c \bmod p$$

- 4 Alicja wysyła A do Boba, Bob wysyła B do Karola, Karol wysyła C do Alicji.

Rozszerzony algorytm Diffie-Hellman'a, cz. 2

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modułarnego

Generator grupy mnożnikowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

- 1 Alicja oblicza: $A' = C^a \text{ mod } p,$
- 2 Bob oblicza: $B' = A^b \text{ mod } p,$
- 3 Karol oblicza: $C' = B^c \text{ mod } p,$
- 4 Alicja wysyła A' do Boba, Bob wysyła B' do Karola, Karol wysyła C' do Alicji,
- 5 Alicja oblicza $k_A = C'^a \text{ mod } p = g^{abc} \text{ mod } p,$
- 6 Bob oblicza $k_B = A'^b \text{ mod } p = g^{abc} \text{ mod } p,$
- 7 Karol oblicza $k_C = B'^c \text{ mod } p = g^{abc} \text{ mod } p,$

Klucz tajny wynosi:

$$k = k_A = k_B = k_C = g^{abc} \text{ mod } p$$

Algorytm Diffie-Hellman'a - bezpieczeństwo, cz. 1

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modułarnego

Generator grupy mnożystawowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

Problem Diffiego-Hellmana

Dla:

- danej liczby pierwszej p ,
- generatora g grupy \mathbb{Z}_p^* ,
- elementów $g^a \bmod p$ oraz $g^b \bmod p$,

znaleźć liczbę całkowitą $g^{ab} \bmod p$.

Idea kryptosystemów asymetrycznych, cz.1

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

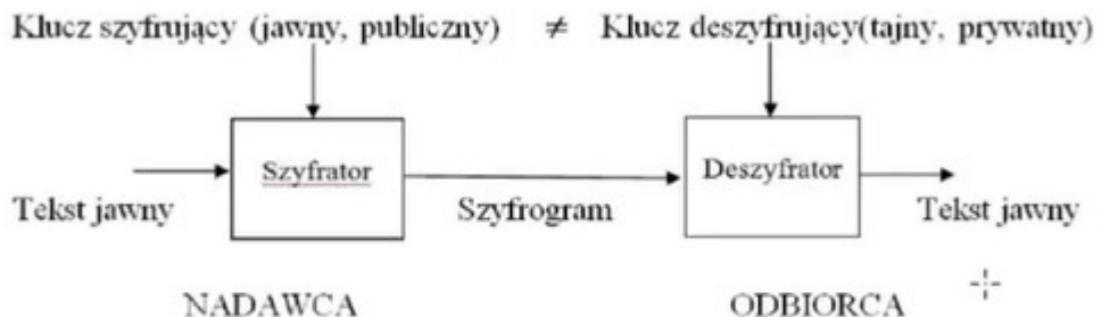
Algorytm szyfrowania potęgowaniem modułarnego

Generator grupy mnożystwowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych



Strony	Klucze publiczne	Klucze prywatne
A	e_A	d_A
B	e_B	d_B

Idea kryptosystemów asymetrycznych, cz.2

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Algorytm
szybkiego
potęgowania
modularnego

Generator grupy
mobilipikatywnej

Logarytm
dyskretny

Protokół
Diffie-Hellman'a

Idea
kryptosystemów
asymetrycznych

Realizacja usługi poufności - szyfrowanie wiadomości przez Alicję:

- 1 Alicja pobiera klucz publiczny Boba e_B .
- 2 Alicja szyfruje wiadomość M kluczem publicznym Boba e_B :

$$C = \text{ENC}_{e_B}(M)$$

- 3 Alicja wysyła do Boba szyfrogram C .

Realizacja usługi poufności - deszyfrowanie szyfrogramu przez Boba:

- 1 Bob otrzymuje od Alicji szyfrogram C .
- 2 Deszyfruje go swoim kluczem prywatnym d_B :

$$M = \text{DEC}_{d_B}(C).$$

Przeciwnik nie może zdeszyfrować wiadomości ponieważ nie zna klucza prywatnego d_B (nie może go wyliczyć na podstawie znajomości klucza publicznego e_B).

Idea kryptosystemów asymetrycznych, cz.3

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modularnego

Generator grupy mnożnikowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

Realizacja usługi uwierzytelnienia - generacja podpisu cyfrowego przez Alicję:

- 1 Alicja chce podpisać wiadomość M podpisem cyfrowym.
- 2 Alicja generuje podpis cyfrowy S za pomocą swojego klucza prywatnego d_A :

$$S = SIG_{d_A}(M).$$

- 3 Alicja wysyła do Boba podpis cyfrowy S oraz wiadomość M .

Idea kryptosystemów asymetrycznych, cz.4

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modułarnego

Generator grupy mnożkowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

Realizacja usługi uwierzytelnienia - weryfikacja podpisu cyfrowego przez Boba:

- 1 Bob otrzymuje od Alicji podpis cyfrowy S oraz wiadomość M .
- 2 Bob weryfikuje podpis cyfrowy kluczem publicznym Alicji e_A :

$$M' = \text{VER}_{e_A}(S).$$

- 3 Jeżeli wyznaczona wiadomość M' jest identyczna z wiadomością otrzymaną M to tożsamość Alicji została poprawnie zweryfikowana, w przeciwnym przypadku tożsamość Alicji nie została poprawnie zweryfikowana.

Uwierzytelniony algorytm D-H

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

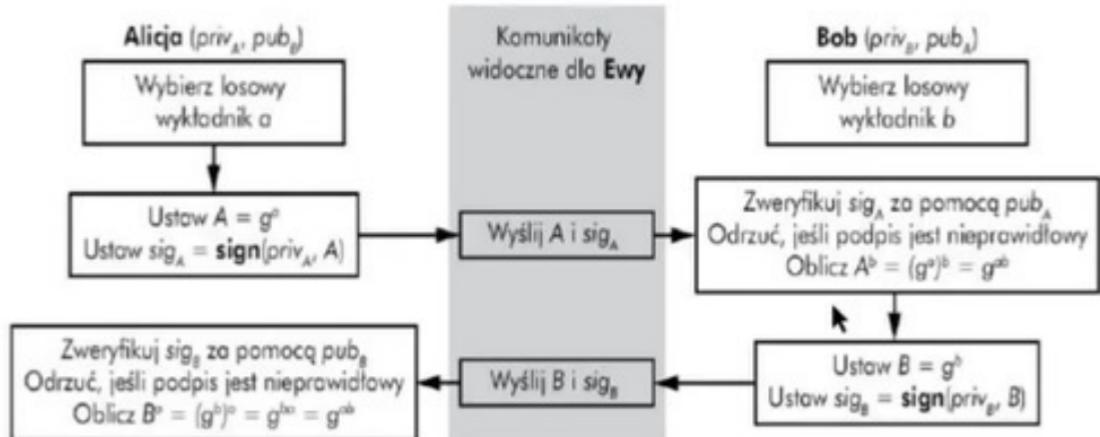
Algorytm szybkiego potęgowania modułowego

Generator grupy mnożnikowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych



Protokół Menezes-Qu-Vanstone - MQV

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modularnego

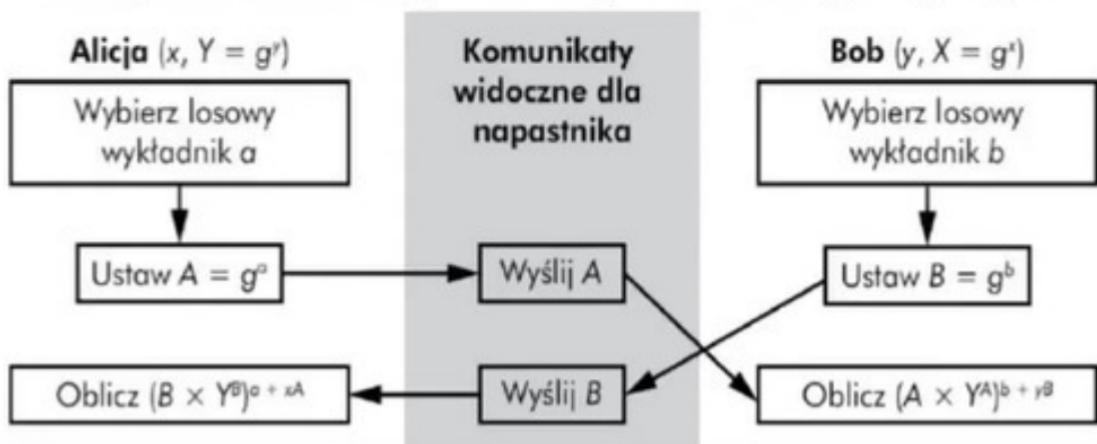
Generator grupy mnożkowej

Algorytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

- Zaprojektowany w 1998 i zatwierdzony przez NSA do ochrony najbardziej krytycznych zasobów; I
- Bardziej bezpieczny niż uwierzytelniony algorytm D-H;
- Używa działań z długoterminowymi kluczami symetrycznymi.



Uwierzytelniony algorytm D-H

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

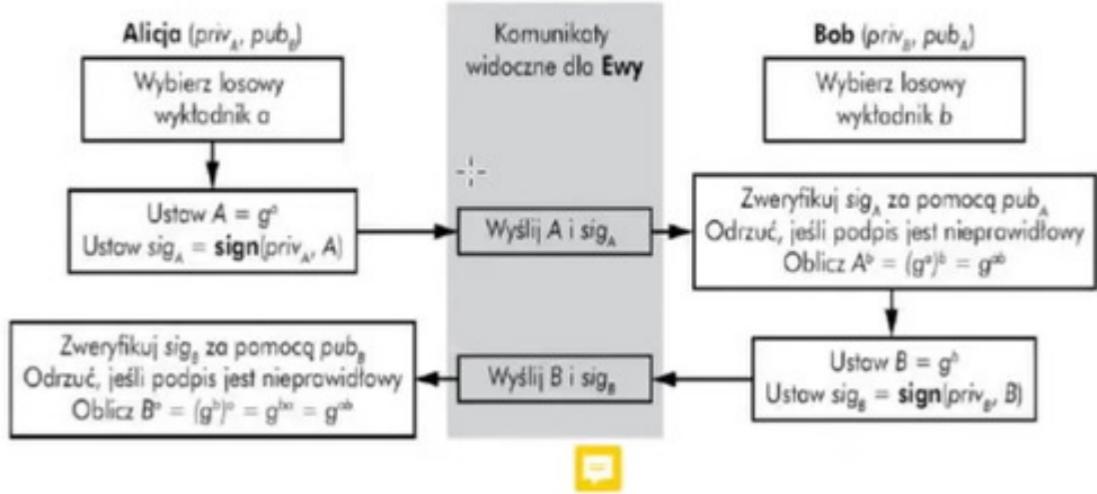
Algorytm szybkiego potęgowania modułarnego

Generator grupy mnożkowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych



Protokół Menezes-Qu-Vanstone - MQV

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Algorytm szybkiego potęgowania modularnego

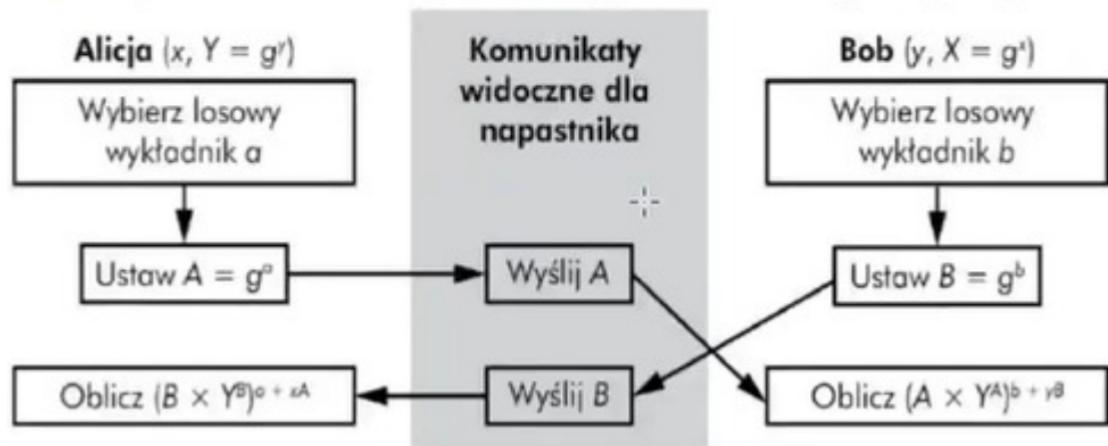
Generator grupy mnożkowej

Logarytm dyskretny

Protokół Diffie-Hellman'a

Idea kryptosystemów asymetrycznych

- Zaprojektowany w 1998 i zatwierdzony przez NSA do ochrony najbardziej krytycznych zasobów;
- Bardziej bezpieczny niż uwierzytelniony algorytm D-H;
- Używa działań z długoterminowymi kluczami symetrycznymi.



Plan wykładu

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mirczański

Wprowadzenie

Histo
kryptosystemów asymetrycznych

Podpis cyfrowy - schemat ogólny

Kryptosystem RSA

Kryptosystem ElGamala, 1985 r.

- 1 Idea kryptosystemów asymetrycznych**
- 2 Podpis cyfrowy**
- 3 Kryptosystem RSA:**
 - Generacja kluczy RSA.
 - Szyfrowanie/deszyfrowanie RSA.
 - Podpis cyfrowy RSA.
- 4 Kryptosystem ElGamala:**
 - Generacja kluczy ElGamala.
 - Szyfrowanie/deszyfrowanie ElGamala.
 - Podpis cyfrowy ElGamala.

WSTĘP DO KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Kryptografia asymetryczna kryptografia klucza publicznego

dr inż. Piotr Mroczkowski

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.



1 Idea kryptosystemów asymetrycznych

2 Podpis cyfrowy

3 Kryptosystem RSA:

- Generacja kluczy RSA.
- Szyfrowanie/deszyfrowanie RSA.
- Podpis cyfrowy RSA.

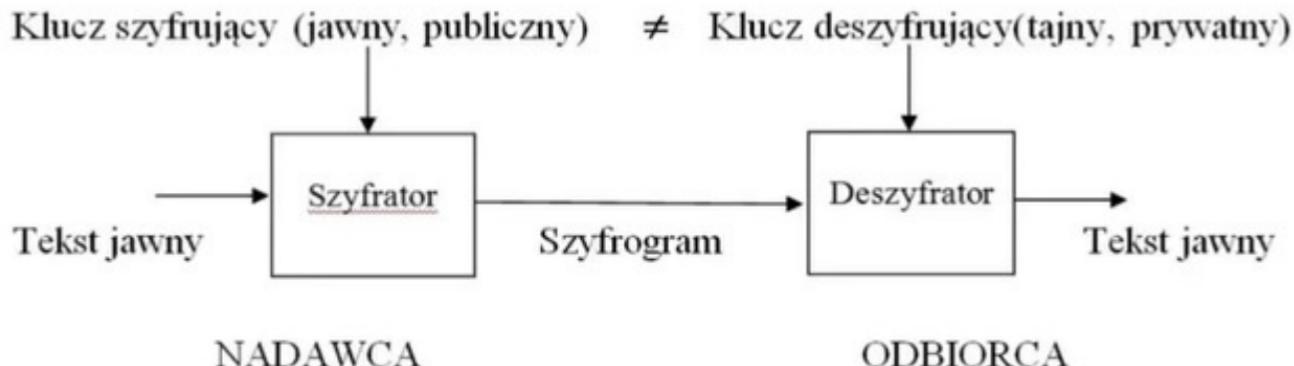
4 Kryptosystem ElGamala:

- Generacja kluczy ElGamala.
- Szyfrowanie/deszyfrowanie ElGamala.
- Podpis cyfrowy ElGamala.

Idea kryptosystemów asymetrycznych, cz. 1

WSTĘP DO
KRYPTOLOGII

Idea kryptosystemów asymetrycznych



Strony	Klucze publiczne	Klucze prywatne
A	e_A	d_A
B	$\overset{\rightarrow}{e_B}$	d_B

Realizacja usługi poufności - szyfrowanie wiadomości przez Alicję:

- 1 Alicja pobiera klucz publiczny Boba e_B .
- 2 Alicja szyfruje wiadomość M kluczem publicznym Boba e_B :

$$C = \text{ENC}_{e_B}(M)$$

- 3 Alicja wysyła do Boba szyfrogram C .

Realizacja usługi poufności - deszyfrowanie szyfrogramu przez Boba:

- 1 Bob otrzymuje od Alicji szyfrogram C .
- 2 Deszyfruje go swoim kluczem prywatnym d_B :

$$M = \text{DEC}_{d_B}(C).$$

Przeciwnik nie może zdeszyfrować wiadomości ponieważ nie zna klucza prywatnego d_B (nie może go wyliczyć na podstawie znajomości klucza publicznego e_B).

Realizacja usługi uwierzytelnienia - generacja podpisu cyfrowego przez Alicję:

- 1 Alicja chce podpisać wiadomość M podpisem cyfrowym.
- 2 Alicja generuje podpis cyfrowy S za pomocą swojego klucza prywatnego d_A :

$$S = \text{SIG}_{d_A}(M).$$

- 3 Alicja wysyła do Boba podpis cyfrowy S^I oraz wiadomość M .

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Podpis ręczny	Podpis cyfrowy
Cechy wspólne	
1. Przypisany jednej osobie	
2. Niemożliwy do podrobienia	
3. Uniemożliwiający wyparcie się go przez autora	
4. Łatwy do weryfikacji przez osobę niezależną	
5. Łatwy do wygenerowania	
Różnice	
6. Związany nierozerlacznie z dokumentem	6. Może być składowany i transmitowany niezależnie od dokumentu
7. Taki sam dla wszystkich dokumentów	7. Jest funkcją dokumentu
8. Tylko na ostatniej stronie dokumentu	8. Obejmuje cały dokument

Realizacja usługi uwierzytelnienia - generacja podpisu cyfrowego przez Alicję:

- 1 Alicja chce podpisać wiadomość M podpisem cyfrowym.
- 2 Alicja generuje podpis cyfrowy S za pomocą swojego klucza prywatnego d_A :

$$S = \text{SIG}_{d_A}(M).$$

- 3 Alicja wysyła do Boba podpis cyfrowy S oraz wiadomość M .

Realizacja usługi uwierzytelnienia - weryfikacja podpisu cyfrowego przez Boba:

- 1 Bob otrzymuje od Alicji podpis cyfrowy S oraz wiadomość M .
- 2 Bob weryfikuje podpis cyfrowy kluczem publicznym Alicji e_A :

$$M' = \text{VER}_{e_A}(S).$$

- 3 Jeżeli wyznaczona wiadomość M' jest identyczna z wiadomością otrzymaną M to tożsamość Alicji została poprawnie zweryfikowana, w przeciwnym przypadku tożsamość Alicji nie została poprawnie zweryfikowana.

Podpis cyfrowy

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Podpis cyfrowy

protokół kryptograficzny realizujący następujące usługi kryptograficzne:

- 1 uwierzytelnienie,
- 2 integralność danych,
- 3 niezaprzeczalność.

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Podpis ręczny	Podpis cyfrowy
Cechy wspólne	
	<ol style="list-style-type: none">1. Przypisany jednej osobie2. Niemożliwy do podrobienia3. Uniemożliwiający wyparcie się go przez autora4. Latwy do weryfikacji przez osobę niezależną5. Latwy do wygenerowania
Różnice	
<ol style="list-style-type: none">6. Związany nieroziącznie z dokumentem7. Taki sam dla wszystkich dokumentów8. Tylko na ostatniej stronie dokumentu	<ol style="list-style-type: none">6. Może być składowany i transmitowany niezależnie od dokumentu7. Jest funkcją dokumentu8. Obejmuje cały dokument

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kyptosystem
RSA

Kyptosystem
ElGamala, 1985 r.

Kryptosystem RSA

Jeden z pierwszych i obecnie najpopularniejszy, asymetryczny algorytm kryptograficzny, zaprojektowany w 1977 przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana. Jego nazwa pochodzi od pierwszych liter nazwisk jego twórców.



Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Podpis ręczny	Podpis cyfrowy
Cechy wspólne	
1. Przypisany jednej osobie	
2. Niemożliwy do podrobienia	
3. Uniemożliwiający wyparcie się go przez autora	
4. Łatwy do weryfikacji przez osobę niezależną	
5. Łatwy do wygenerowania	
Różnice	
6. Związany nierozięcznie z dokumentem	6. Może być składowany i transmitowany niezależnie od dokumentu
7. Taki sam dla wszystkich dokumentów	7. Jest funkcją dokumentu
8. Tylko na ostatniej stronie dokumentu	8. Obejmuje cały dokument

Kryptosystem RSA

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kyptosystem
RSA

Kyptosystem
ElGamala, 1985 r

Kryptosystem RSA

Jeden z pierwszych i obecnie najpopularniejszy, asymetryczny algorytm kryptograficzny, zaprojektowany w 1977 przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana. Jego nazwa pochodzi od pierwszych liter nazwisk jego twórców.

Kryptosystem RSA

Jeden z pierwszych i obecnie najpopularniejszy, asymetryczny algorytm kryptograficzny, zaprojektowany w 1977 przez Rona Rivesta, Adi Shamira oraz Leonarda Adlemana. Jego nazwa pochodzi od pierwszych liter nazwisk jego twórców.

■ Zastosowanie:

- 1 zapewnienie poufności
- 2 zapewnienie uwierzytelnienia

■ Bezpieczeństwo

kryptosystemu oparte jest na trudności faktoryzacji dużych liczb złożonych.



Kryptosystem RSA - generacja kluczy RSA

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Idea kryptosystemów asymetrycznych

Podpis cyfrowy - schemat ogólny

Kryptosystem RSA

Kryptosystem ElGamala, 1985 r.

- 1 Wygenerować losowo dwie duże, różne liczby pierwsze p i q .
- 2 Obliczyć $n = pq$ oraz $\phi = (p - 1)(q - 1)$.
- 3 Wybrać losowo liczbę całkowitą e , $1 < e < \phi$, taką że $\gcd(e, \phi) = 1$.
- 4 Korzystając z rozszerzonego algorytmu Euclidesa wyznaczyć liczbę $d = e^{-1} \bmod \phi$ (d jest odwrotnością multiplikatywną e modulo ϕ).
- 5 Wyznaczone klucze:
 - $k_1 = (e, n)$ - klucz publiczny,
 - $k_2 = (d, n)$ - klucz prywatny.
- 6 Liczby p, q, ϕ są kasowane.

Kryptosystem RSA - generacja kluczy RSA

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Idea kryptosystemów asymetrycznych

Podpis cyfrowy - schemat ogólny

Kryptosystem RSA

Kryptosystem ElGamala, 1985 r.

Przykład: Generacja kluczy przez Alicję:

- Alicja:
 - 1 wybiera dwie liczby pierwsze: $p = 13$ oraz $q = 17$,
 - 2 oblicza: $n = pq = 13 \cdot 17 = 221$ oraz
 $\phi = (p - 1)(q - 1) = 12 \cdot 16 = 192$,
 - 3 wybiera: $e = 151$,
 - 4 korzystając z rozszerzonego algorytmu Euklidesa oblicza
 $d = e^{-1} \bmod \phi = 151^{-1} \bmod 192 = 103$.
- Kluczem publicznym Alicji jest para: $k_1 \stackrel{\text{I}}{=} (e, n) = (151, 221)$,
- Kluczem prywatnym Alicji jest para: $k_2 = (d, n) = (103, 221)$,

Kryptosystem RSA - etap poufnej wymiany informacji



WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Niech:

- $k_1 = (e, n)$ - klucz publiczny,
- $k_2 = (d, n)$ - klucz prywatny,
- $x \in Z_n$ - liczba będąca wiadomością do zaszyfrowania,

1 Szyfrowanie:

$$y = E_{k_1}(x) = x^e \bmod n$$

2 Deszyfrowanie:

$$x = D_{k_2}(y) = y^d \bmod n$$

Kryptosystem RSA - dowód poprawności

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Należy wykazać, że:

$$D_{k_2}(E_{k_1}(m)) = m$$

- $m = c^d \bmod n = (m^e)^d \bmod n = m^{ed} \bmod n,$
- ponieważ $ed \bmod \phi = 1$, to $ed \equiv 1 \bmod \phi$ z której wynika $\phi|(ed - 1)$,
- istnieje liczba całkowita k taka, że $ed - 1 = k \cdot \phi$,
- dostajemy $ed = k \cdot \phi + 1$,
- $m = m^{ed} \bmod n = m^{k \cdot \phi + 1} \bmod n = m \cdot (m^\phi)^k \bmod n = m \cdot (1)^k \bmod n = m$

Problem RSA

Dla danych:

- dodatniej liczby całkowitej $n = p \cdot q$, będącej iloczynem dwóch różnych liczb pierwszych p i q ,
- dodatniej liczby całkowitej e takiej, że $\gcd(e, (p-1)(q-1)) = 1$,
- liczby całkowitej c .

znaleźć liczbę całkowitą m taką, że $m^e \pmod{n} = c$.

Inaczej mówiąc, problem RSA polega na:

- odtworzeniu tekstu jawnego m na podstawie odpowiadającego mu szyfrogramu c , przy założeniu znajomości klucza publicznego $k_1 = (e, n)$ właściwego odbiorcy wiadomości i nie znajomości klucza publicznego $k_2 = (d, n)$ właściwego odbiorcy wiadomości.

Szyfrownie RSA w praktyce:

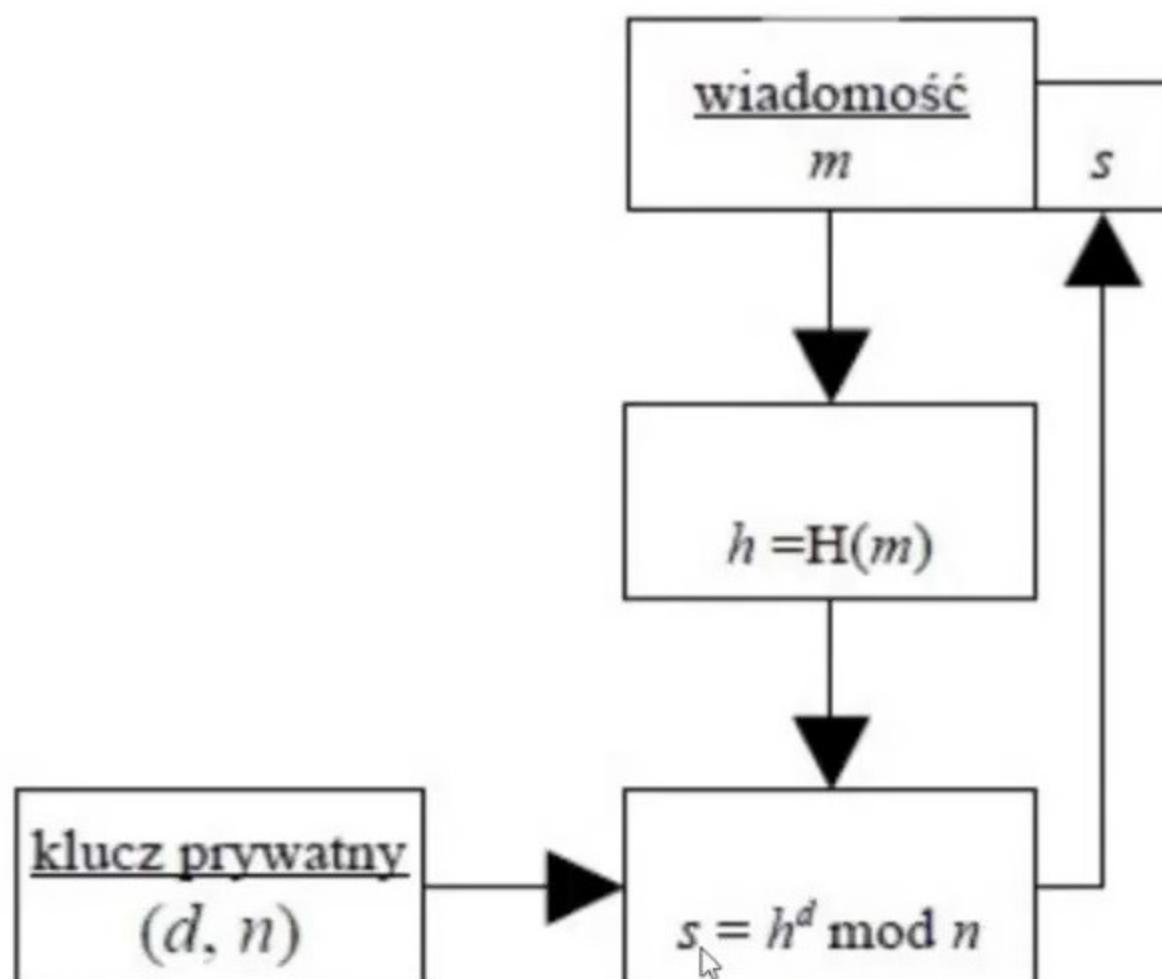
- długość modułu n : min. 2048 bity,
- wybieranie liczb pierwszych p i q :
 - rozkład $n = pq$ na czynniki pierwsze był obliczeniowo niewykonalny,
 - liczby p i q powinny mieć w przybliżeniu taką samą długość w bitach, np. jeśli jest stosowany 2048-bitowy moduł n , to p i q powinny mieć w przybliżeniu po 1024 bitów,
 - liczby p i q powinny być mocnymi liczbami pierwszymi

Definicja

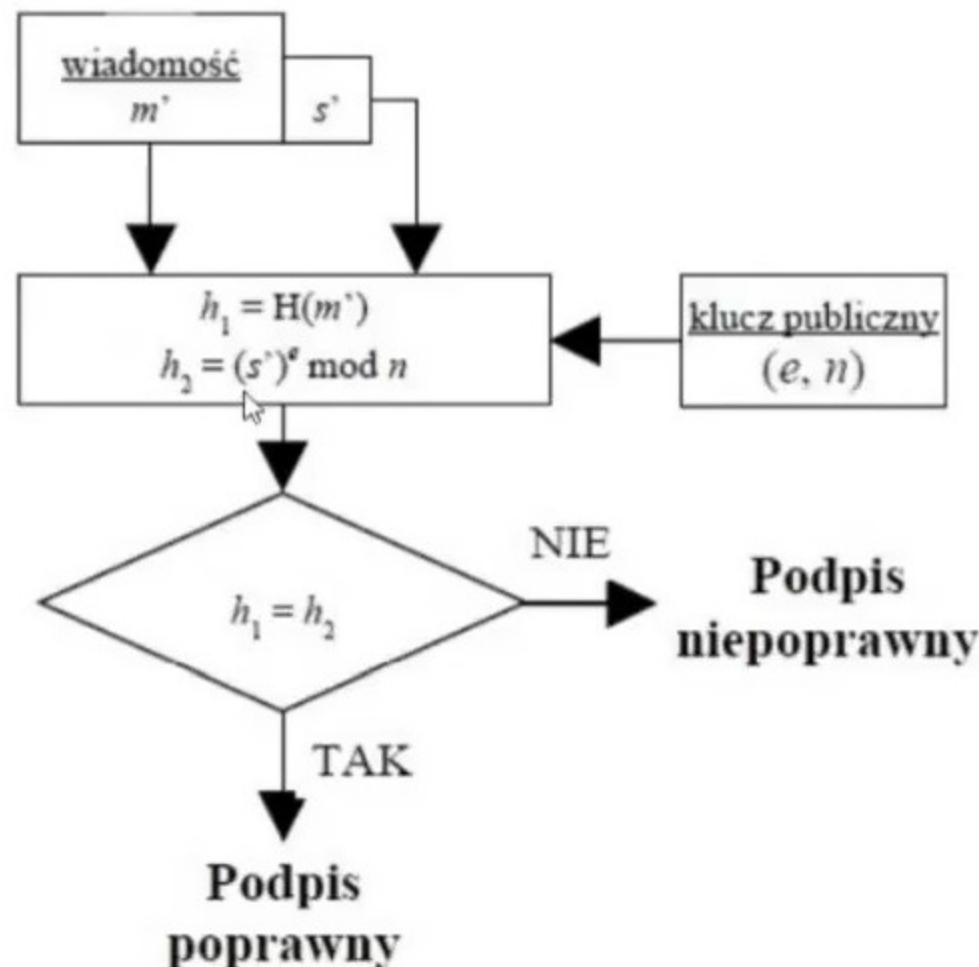
Liczby pierwsze p i q nazywamy **mocnymi liczbami pierwszymi**, gdy:

- największy wspólny dzielnik liczb $p-1$ i $q-1$ powinien być mały,
- liczby $p-1$ i $q-1$ powinny mieć duże czynniki pierwsze,
- liczby $(p-1)/2$ i $(q-1)/2$ powinny być pierwszymi.

Niech dana będzie wiadomość m , klucz prywatny $k_2 = (d, n)$ oraz funkcja skrótu H .



- 1 Wyznaczenie skrótu wiadomości $h = H(m)$.
- 2 Obliczenie $s = h^d \bmod n$.
- 3 Podpisem wiadomości m jest s .

Strona B odbiera wiadomość m' wraz z podpisem s' 

- 1 Wyznaczenie skrótu wiadomości $h_1 = H(m')$.
- 2 Obliczenie $h_2 = (s')^e \text{ mod } n$.
- 3 Sprawdzenie, czy $h_1 = h_2$ (warunek podpisu).
- 4 Jeśli $h_1 = h_2$ podpis poprawny, w p.p. podpis niepoprawny.

1 Generacja podpisu cyfrowego Alicji:

- m będzie wiadomością, której skrót wynosi $h = H(m) = 25$.
- $k_2 = (d, n) = (103, 221)$ - klucz prywatny Alicji.
- Alicja wyznacza podpis cyfrowy:

$$s = h^d \bmod n = 25^{103} \bmod 221 = 168$$

2 Weryfikacja podpisu przez Boba:

- pobiera klucz publiczny Alicji $k_1 = (e, n) = (151, 221)$,
- otrzymuje wiadomość m' wraz z podpisem $s' = 168$.
- wyznacza skrót z otrzymanej wiadomości m' przy użyciu f. skrótu: $h_1 = H(m') = 25$.
- oblicza skrót przy użyciu klucza publicznego Alicji:

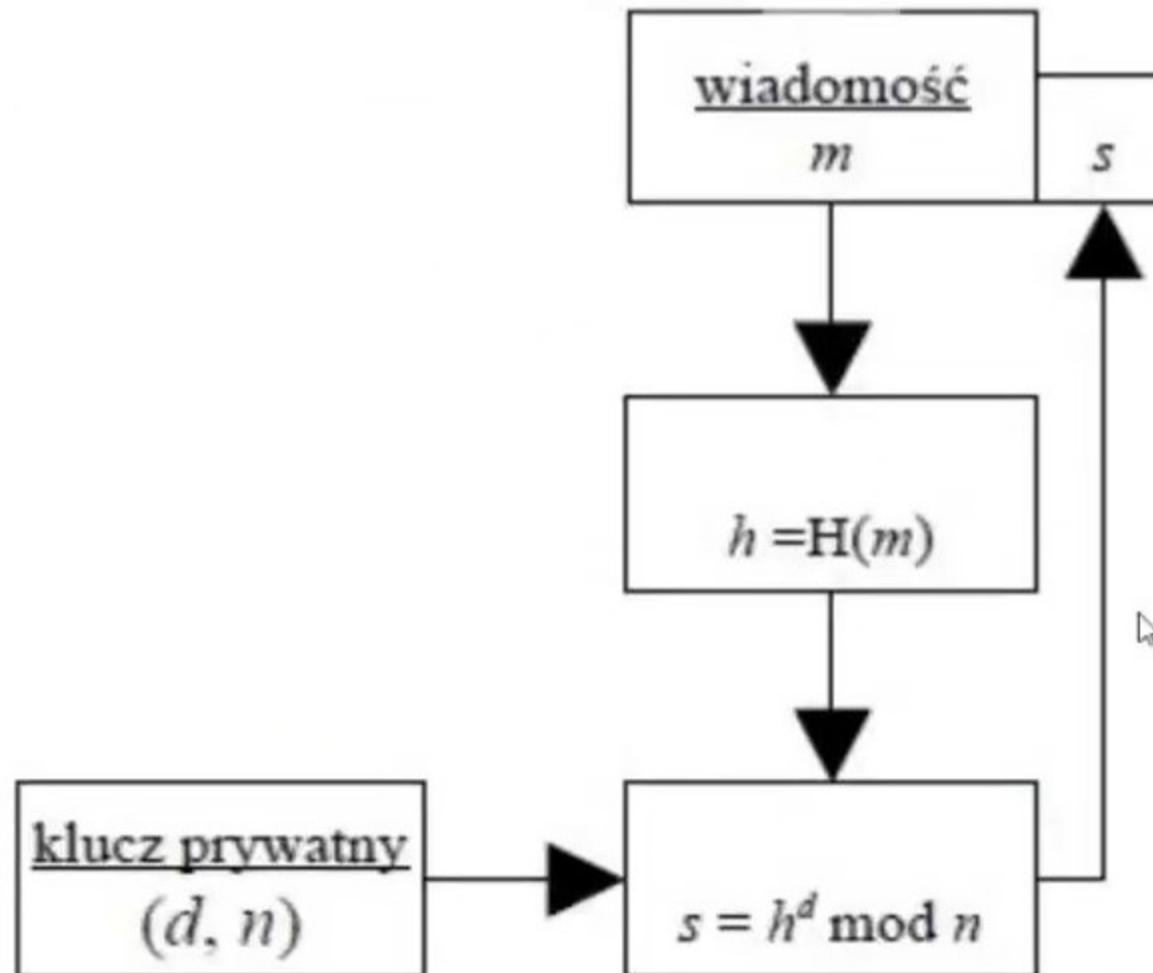
$$h_2 = (s')^e \bmod n = 168^{151} \bmod 221 = 25$$

I

- ponieważ $h_1 = h_2 = 25$ - podpis prawidłowy.

Podpis cyfrowy RSA - generacja podpisu

Niech dana będzie wiadomość m , klucz prywatny $k_2 = (d, n)$ oraz funkcja skrótu H .



Kryptosystem RSA - warunki bezpieczeństwa

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Idea kryptosystemów asymetrycznych

Podpis cyfrowy - schemat ogólny

Kryptosystem RSA

Kryptosystem ElGamala, 1985 r.

Szyfrownie RSA w praktyce:

- długość modułu n : min. 2048 bity,
- wybieranie liczb pierwszych p i q :
 - rozkład $n = pq$ na czynniki pierwsze był obliczeniowo niewykonalny,
 - liczby p i q powinny mieć w przybliżeniu taką samą długość w bitach, np. jeśli jest stosowany 2048-bitowy moduł n , to p i q powinny mieć w przybliżeniu po 1024 bitów,
 - liczby p i q powinny być mocnymi liczbami pierwszymi

Definicja

Liczby pierwsze p i q nazywamy **mocnymi liczbami pierwszymi**, gdy:

- największy wspólny dzielnik liczb $p-1$ i $q-1$ powinien być mały,
- liczby $p-1$ i $q-1$ powinny mieć duże czynniki pierwsze,
- liczby $(p-1)/2$ i $(q-1)/2$ powinny być pierwszymi.

Kryptosystem ElGamala

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Kryptosystem ElGamala

Jeden z najważniejszych (obok RSA) kryptosystemów asymetrycznych. Zaprojektowany w 1985 przez Egipcjanina Tahera ElGamala.

- Zastosowanie:
 - 1 zapewnienie poufności
 - 2 zapewnienie uwierzytelnienia
- Bezpieczeństwo kryptosystemu oparte jest na trudności obliczania logarytmów dyskretnych w ciele liczb całkowitych modulo duża liczba pierwsza.
- Każdorazowe szyfrowanie wykorzystuje losowo wygenerowaną liczbę (ten sam tekst jawnny daje inny kryptogram).
- Szyfrogramy są dwukrotnie dłuższe niż tekst jawnie.



Kryptosystem ElGamala - generacja kluczy

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Idea kryptosystemów asymetrycznych

Podpis cyfrowy - schemat ogólny

Kryptosystem RSA

Kryptosystem ElGamala, 1985 r.

- 1 Wygenerować losowo taką dużą liczbę pierwszą p taką, aby obliczenie logarytmów dyskretnych modulo p było praktycznie niewykonalne.
- 2 Wybrać generator α dla Z_p^* .
- 3 Wybrać losowo liczbę $1 < t < p - 1$ i obliczyć $\beta = \alpha^t \bmod p$.
- 4 Klucz $k_1 = (p, \alpha, \beta)$ jest kluczem publicznym, klucz $k_2 = (p, t)$ jest kluczem prywatnym.

Kryptosystem ElGamala - etap poufnej wymiany informacji

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Idea kryptosystemów asymetrycznych

Podpis cyfrowy - schemat ogólny

Kryptosystem RSA

Kryptosystem ElGamala, 1985 r.



- 1 Szyfrowanie - strona B szyfruje wiadomość przy użyciu klucza publicznego k_1 strony A.

Niech:

- $P = x \in Z_p$ - liczba będąca wiadomością do zaszyfrowania
- $k_1 = (p, \alpha, \beta)$ - klucz publiczny strony A,
- $1 < r < p - 1$ - randomizer

$$C = (y_1, y_2) = E_{k_1}(r, x) = (\alpha^r \bmod p, x \cdot \beta^r \bmod p)$$

- 2 Deszyfrowanie - strona A deszyfruje otrzymaną wiadomość przy użyciu swojego klucza prywatnego k_2 .

Niech:

- $C = (y_1, y_2)$, gdzie $y_1, y_2 \in Z_p$ - liczby będące kryptogramem do zdeszyfrowania,
- $k_2 = (p, t)$ - klucz prywatny strony A.

$$P = x = D_{k_2}(y_1, y_2) = y_2 \cdot (y_1^t)^{-1} \bmod p = y_2 \cdot y_1^{p-1-t} \bmod p$$

Kryptosystem ElGamala - dowód poprawności

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

■
Kryptosystem
ElGamala, 1985 r.

Należy wykazać, że:

$$x = D_{k_2}(E_{k_1}(x)) \quad \rightarrow$$

$$y_2 \cdot (y_1^t)^{-1} \bmod p = x \cdot \beta^r \cdot (\alpha^{rt})^{-1} \bmod p = x \cdot \alpha^{rt} \cdot (\alpha^{rt})^{-1} \bmod p = x$$

Kryptosystem ElGamala - etap poufnej wymiany informacji

WSTĘP DO KRYPTOLOGII

dr inż. Piotr Mroczkowski

Wprowadzenie

Idea kryptosystemów asymetrycznych

Podpis cyfrowy - schemat ogólny

Kryptosystem RSA

Kryptosystem ElGamala, 1985 r.

Przykład:

Niech: $x = 20$, $r = 10$.

- Bob przy użyciu klucza $k_1 = (p, \alpha, \beta) = (101, 2, 100)$ oblicza:

$$(y_1, y_2) = (\alpha^r \bmod p, x \cdot \beta^r \bmod p) =$$

$$(2^{10} \bmod 101, 20 \cdot 100^{10} \bmod 101) = (14, 20)$$

- Alicja przy użycia klucza $k_2 = (p, t) = (101, 50)$ oblicza:

$$x = y_2 \cdot y_1^{p-1-t} \bmod p =$$

$$20 \cdot 14^{101-1-50} \bmod 101 = 20 \cdot 14^{50} \bmod 101 = 20$$

Kryptosystem ElGamala - bezpieczeństwo

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Problem ElGamala

Dla danych:

- liczby pierwszej p ,
- generatora α grupy Z_p^* ,
- elementu $\beta \in Z_p^*$,

znać liczbę całkowitą x , $0 \leq x \leq p-2$ taką, że $\alpha^x \equiv \beta \pmod{p}$.

Inaczej mówiąc, bezpieczeństwo algorytmu ElGamala opiera się na:

- trudności obliczenia tajnej wartości t niezbędnej do odszyfrowania wiadomości z powszechnie znanej wartości $\beta = \alpha^t \pmod{p}$,

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Biorąc pod uwagę ostatnie osiągnięcia w dziedzinie rozwiązywania problemu logarytmu dyskretnego w Z_p^* moduł p powinien być liczbą min. 2048 bitów.



Podpis cyfrowy ElGamala - generacja podpisu

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

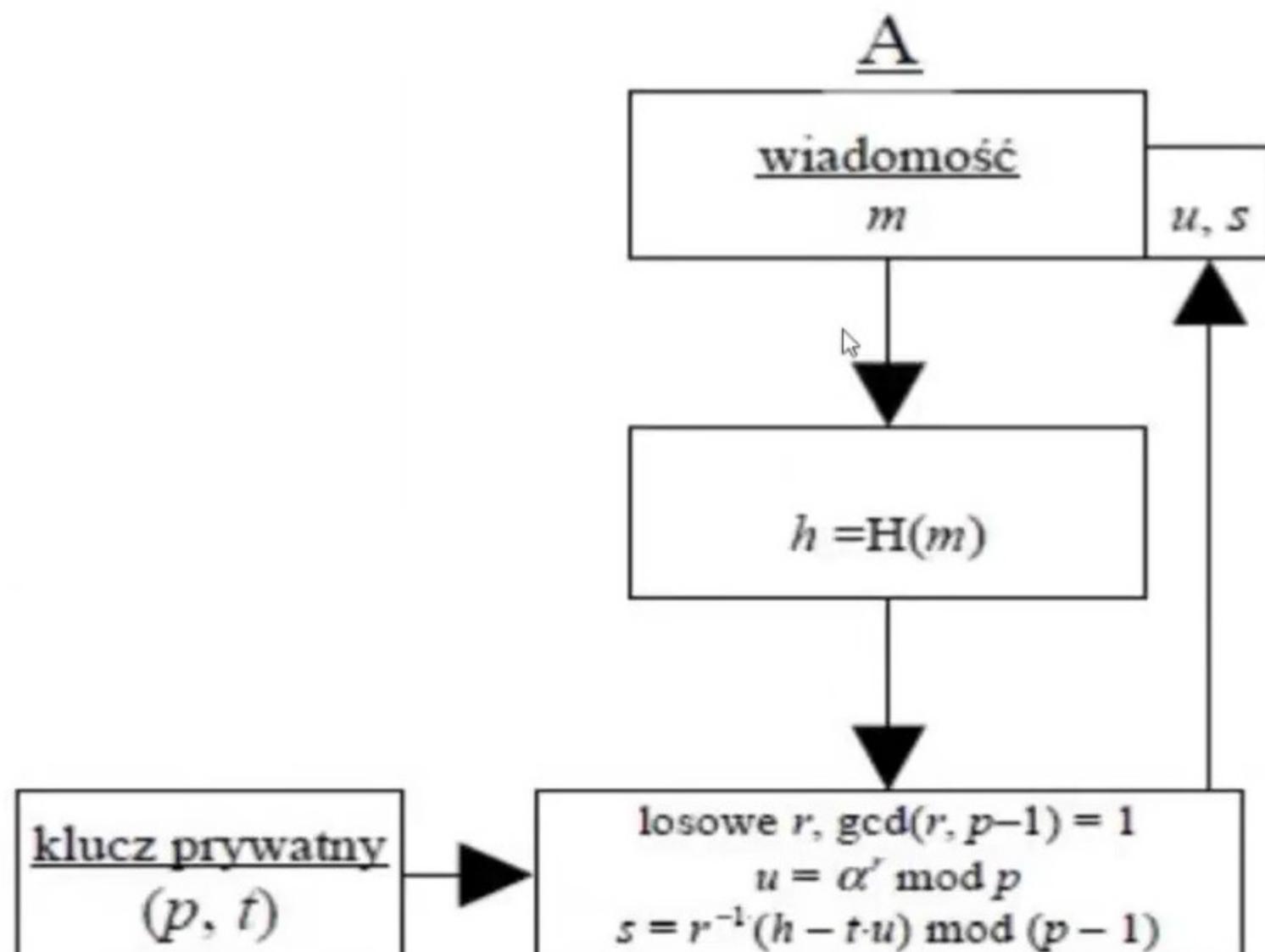
Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Dane wejściowe: wiadomość m , klucz prywatny strony A: $k_2 = (p, t)$ oraz funkcja skrótu H .
Dane wyjściowe: podpis (u, s) .



Podpis cyfrowy ElGamala - generacja podpisu

WSTĘP DO
KRYPTOLOGII

dr inż. Piotr
Mroczkowski

Wprowadzenie

Idea
kryptosystemów
asymetrycznych

Podpis cyfrowy -
schemat ogólny

Kryptosystem
RSA

Kryptosystem
ElGamala, 1985 r.

Dane wejściowe: wiadomość m , klucz prywatny strony A: $k_2 = (p, t)$ oraz f. skrótu H .

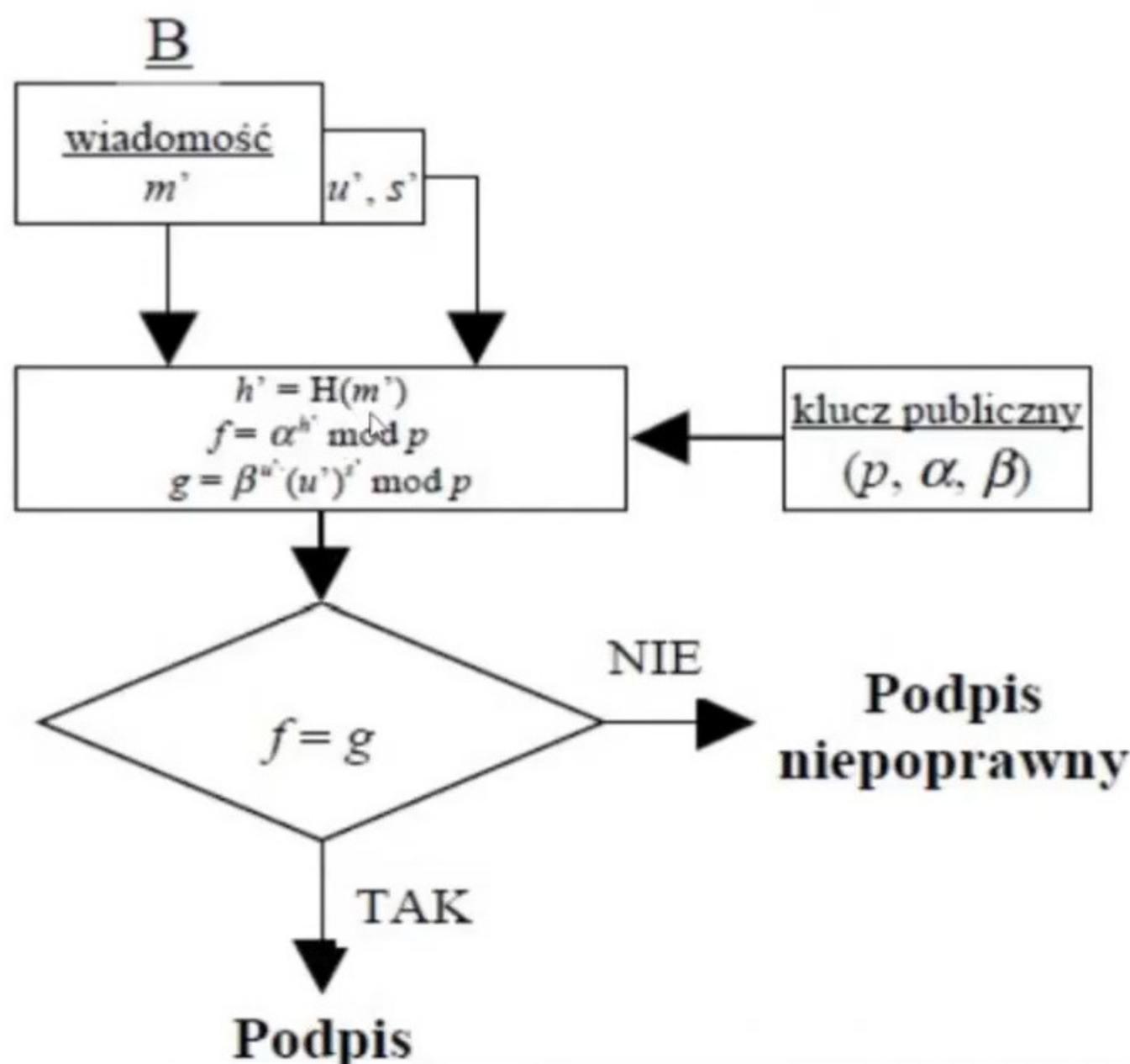
Dane wyjściowe: podpis (u, s) .

- 1 Wyznaczenie skrótu z wiadomości $h = H(m)$.
- 2 Wybieranie losowo liczbę r taką, że $1 < r < p - 1$ oraz $\gcd(r, p - 1) = 1$.
- 3 Obliczenie $u = \alpha^r \bmod p$.
- 4 Obliczenie $r^{-1} \bmod (p - 1)$.
- 5 Obliczenie $s = r^{-1} \cdot (h - t \cdot u) \bmod (p - 1)$.
- 6 Podpisem wiadomości m jest para liczb (u, s) .
- 7 Wysyłanie do B wiadomości m wraz z podpisem (u, s) .

Podpis cyfrowy ElGamala - weryfikacja podpisu

Dane wejściowe:

- klucz publiczny strony A: $k_1 = (p, \alpha, \beta)$,
- wiadomość: $m' = m$, podpis: $(u', s') = (u, s)$



Dane wejściowe:

- klucz publiczny strony A: $k_1 = (p, \alpha, \beta)$,
 - wiadomość: $m' = m$, podpis: $(u', s') = (u, s)$
- 1 Odebranie wiadomości m' wraz z podpisem (u', s')
 - 2 Wyznaczenie skrótu wiadomości $h' = H(m')$.
 - 3 Obliczenie $f = (\alpha)^{h'} \text{ mod } p$.
 - 4 Obliczenie $g = (\beta)^{u'} \cdot (u')^{s'} \text{ mod } p$.
 - 5 Sprawdzenie, czy $f = g$ (warunek weryfikacji podpisu).
 - 6 Jeśli $f = g$ podpis poprawny, w p.p podpis niepoprawny.

Weryfikacja podpisu - strona B

- posiada klucz publiczny strony A: $k_1 = (p, \alpha, \beta) = (101, 2, 100)$,
- otrzymała wiadomość m' wraz z podpisem $(u', s') = (98, 80)$.
- wyznacza skrót z otrzymanej wiadomości m' przy użyciu f.
skrótu: $h' = H(m') = 20$.
- oblicza wartość funkcji f i g przy użyciu klucza publicznego
strony A: