Kryptografia współczesna

Janusz Słupik

Politechnika Śląska

Wydział Matematyczno-Fizyczny

13 listopada 2009

Wada systemów klasycznych:
Konieczność spotkania się w celu ustalenia i wymiany kluczy szyfrujących i deszyfrujących.

Idea:
Większość współczesnych systemów kryptograficznych jest budowana w oparciu o problemy matematyczne i obliczeniowe.

Liczby pierwsze

Zbiór liczb naturalnych

$$\mathbb{N} = \{1, 2, 3, \ldots\} .$$

Liczbę naturalną $p > 1$ nazywamy **liczbą pierwszą** jeśli jest ona podzielna tylko przez 1 oraz samą siebie.

Zbiór liczb pierwszych:

$$\mathcal{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots\} .$$

Zbiór $\mathcal{P}$ jest nieskończony.

Rozkład liczb naturalnych

Twierdzenie

Każdą liczbę naturalną $n \in \mathbb{N}$ $(n > 1)$ można rozłożyć na iloczyn liczb pierwszych jednoznacznie z dokładnością do kolejności czynników.

Przykład.

$$364 = 2 \cdot 2 \cdot 7 \cdot 13$$

Rozkład liczb naturalnych

Twierdzenie

Każdą liczbę naturalną $n \in \mathbb{N}$ $(n > 1)$ można rozłożyć na iloczyn liczb pierwszych jednoznacznie z dokładnością do kolejności czynników.

Przykład.

$$364 = 2 \cdot 2 \cdot 7 \cdot 13$$

Problem: rozkład dużych liczb naturalnych w krótkim czasie

„Rzut monetą przez telefon”

Rzut monetą to popularna metoda rozstrzygania sporów lub wyboru jednej z dwóch możliwości. Metody tej nie da się zastosować w sytuacji gdy spór toczy się pomiędzy dwoma osobami w dużej odległości. Ta strona, która faktycznie ma przy sobie monetę może skłamać co do wyniku rzutu.

Istnieje kryptograficzny algorytm umożliwiający uzyskanie uczciwego rzutu monetą w takiej sytuacji.

„Rzut monetą przez telefon” - algorytm

1. Strona A wybiera dwie duże liczby pierwsze p i q, albo obie przystające do $1 \pmod 4$, albo obie przystające do $3 \pmod 4$.

„Rzut monetą przez telefon” - algorytm

1. Strona A wybiera dwie duże liczby pierwsze p i q, albo obie przystające do 1 (mod 4), albo obie przystające do 3 (mod 4).
2. Strona A przekazuje stronie B wynik mnożenia tych dwóch liczb: $N = pq$, zachowując p i q w tajemnicy. Można łatwo udowodnić, że N zawsze będzie przystawało do 1 (mod 4). Wybrane liczby muszą być na tyle duże, aby rozkład N był niewykonalny dla strony B w czasie przeznaczonym na wykonanie następnego kroku.

„Rzut monetą przez telefon” - algorytm

1. Strona A wybiera dwie duże liczby pierwsze p i q, albo obie przystające do 1 (mod 4), albo obie przystające do 3 (mod 4).
2. Strona A przekazuje stronie B wynik mnożenia tych dwóch liczb: $N = pq$, zachowując p i q w tajemnicy. Można łatwo udowodnić, że N zawsze będzie przystawało do 1 (mod 4). Wybrane liczby muszą być na tyle duże, aby rozkład N był niewykonalny dla strony B w czasie przeznaczonym na wykonanie następnego kroku.
3. Strona B wybiera (zgaduje) wynik: "1" albo "3", określając do jakiej liczby przystają p i q modulo 4.

„Rzut monetą przez telefon” - algorytm

1. Strona A wybiera dwie duże liczby pierwsze p i q, albo obie przystające do 1 (mod 4), albo obie przystające do 3 (mod 4).
2. Strona A przekazuje stronie B wynik mnożenia tych dwóch liczb: $N = pq$, zachowując p i q w tajemnicy. Można łatwo udowodnić, że N zawsze będzie przystawało do 1 (mod 4). Wybrane liczby muszą być na tyle duże, aby rozkład N był niewykonalny dla strony B w czasie przeznaczonym na wykonanie następnego kroku.
3. Strona B wybiera (zgaduje) wynik: "1" albo "3", określając do jakiej liczby przystają p i q modulo 4.
4. Strona A ogłasza wartości p i q, i czy B odgadła prawidłowo. Strona B może łatwo sprawdzić czy to są prawidłowe liczby sprawdzając czy są pierwsze i mnożąc je przez siebie (jeśli są pierwsze, to N nie ma innych rozkładów na czynniki).

„Rzut monetą przez telefon” - algorytm

1. Strona A wybiera dwie duże liczby pierwsze p i q, albo obie przystające do 1 (mod 4), albo obie przystające do 3 (mod 4).
2. Strona A przekazuje stronie B wynik mnożenia tych dwóch liczb: $N = pq$, zachowując p i q w tajemnicy. Można łatwo udowodnić, że N zawsze będzie przystawało do 1 (mod 4). Wybrane liczby muszą być na tyle duże, aby rozkład N był niewykonalny dla strony B w czasie przeznaczonym na wykonanie następnego kroku.
3. Strona B wybiera (zgaduje) wynik: "1" albo "3", określając do jakiej liczby przystają p i q modulo 4.
4. Strona A ogłasza wartości p i q, i czy B odgadła prawidłowo. Strona B może łatwo sprawdzić czy to są prawidłowe liczby sprawdzając czy są pierwsze i mnożąc je przez siebie (jeśli są pierwsze, to N nie ma innych rozkładów na czynniki).
Stany: B odgadła = „orzeł”, B nie odgadła = „reszka”

Tajne obliczanie średniej

Nauczyciel chce dowiedzieć się, ile czasu przeciętnie poświecają jego uczniowie w ciągu tygodnia zadaniom domowym. Gdyby spytać o to wprost każdego ucznia, wiele odpowiedzi zostałoby zafałszowanych z dwóch powodów:

Tajne obliczanie średniej

Nauczyciel chce dowiedzieć się, ile czasu przeciętnie poświecają jego uczniowie w ciągu tygodnia zadaniom domowym. Gdyby spytać o to wprost każdego ucznia, wiele odpowiedzi zostałoby zafałszowanych z dwóch powodów:

- Uczniowie, którzy poświęcają mało czasu zadaniom domowym mogliby chcieć to ukryć przed nauczycielem.

Tajne obliczanie średniej

Nauczyciel chce dowiedzieć się, ile czasu przeciętnie poświecają jego uczniowie w ciągu tygodnia zadaniom domowym. Gdyby spytać o to wprost każdego ucznia, wiele odpowiedzi zostałoby zafałszowanych z dwóch powodów:

- Uczniowie, którzy poświęcają mało czasu zadaniom domowym mogliby chcieć to ukryć przed nauczycielem.
- Uczniowie poświęcający dużo czasu mogliby nie chcieć tego ujawnić przed kolegami w obawie, że zostaną nazywani „kujonami".

Tajne obliczanie średniej

Nauczyciel chce dowiedzieć się, ile czasu przeciętnie poświecają jego uczniowie w ciągu tygodnia zadaniom domowym. Gdyby spytać o to wprost każdego ucznia, wiele odpowiedzi zostałoby zafałszowanych z dwóch powodów:

- Uczniowie, którzy poświęcają mało czasu zadaniom domowym mogliby chcieć to ukryć przed nauczycielem.
- Uczniowie poświęcający dużo czasu mogliby nie chcieć tego ujawnić przed kolegami w obawie, że zostaną nazywani „kujonami".

Jeżeli nauczyciel jest zainteresowany jedynie informacją o średniej, a nie indywidualnymi danymi, to istnieje procedura pozwalająca wyznaczyć taką średnią w sposób tajny.

Tajne obliczanie średniej - procedura

Uczniowie stają w okręgu.

Tajne obliczanie średniej - procedura

Uczniowie stają w okręgu.

Jedno z nich - Alicja - wybiera w tajemnicy przed innymi losową liczbę. Do tej liczby Alicja dodaje liczbę godzin, którą spędza nad zadaniami domowymi.

Tajne obliczanie średniej - procedura

Uczniowie stają w okręgu.

Jedno z nich - Alicja - wybiera w tajemnicy przed innymi losową liczbę. Do tej liczby Alicja dodaje liczbę godzin, którą spędza nad zadaniami domowymi.

Wynik szepce do ucha uczniowi z prawej strony - Bolkowi. Bolek dodaje liczbę godzin, jaką poświęca zadaniom domowym do liczby, którą usłyszał. Wynik szepce Celinie. Itd.

Tajne obliczanie średniej - procedura

Uczniowie stają w okręgu.

Jedno z nich - Alicja - wybiera w tajemnicy przed innymi losową liczbę. Do tej liczby Alicja dodaje liczbę godzin, którą spędza nad zadaniami domowymi.

Wynik szepce do ucha uczniowi z prawej strony - Bolkowi. Bolek dodaje liczbę godzin, jaką poświęca zadaniom domowym do liczby, którą usłyszał. Wynik szepce Celinie. Itd.

Postępowanie kontynuujemy, aż suma dojdzie z powrotem do Alicji. Ta od otrzymanej sumy odejmuje swoją sekretną liczbę i uzyskany wynik przekazuje nauczycielowi.

Zamiana ciągu liter na liczbę

Jak zamienić ciąg liter długości k na liczbę naturalną?
Odwrotnie, jak zamienić liczbę naturalną na ciąg liter?

Zamiana ciągu liter na liczbę

Jak zamienić ciąg liter długości k na liczbę naturalną?
Odwrotnie, jak zamienić liczbę naturalną na ciąg liter?

Niech X będzie pewnym alfabetem (zbiorem liter).
Załóżmy, że $|X| = n$. Każdej literze przyporządkujemy odpowiednik liczbowy ze zbioru $\{0, 1, \ldots, n-1\}$. Oznaczmy to przyporządkowanie poprzez f.

Zamiana ciągu liter na liczbę

Jak zamienić ciąg liter długości k na liczbę naturalną?
Odwrotnie, jak zamienić liczbę naturalną na ciąg liter?

Niech X będzie pewnym alfabetem (zbiorem liter).
Załóżmy, że $|X| = n$. Każdej literze przyporządkujemy odpowiednik liczbowy ze zbioru $\{0, 1, \ldots, n-1\}$. Oznaczmy to przyporządkowanie poprzez f.

Mamy słowo $u = x_1 x_2 \ldots x_k$, gdzie $x_i \in X$ dla $1 \leqslant i \leqslant k$. Wtedy

$$u \longleftrightarrow f(x_1) + f(x_2) \cdot n + f(x_3) \cdot n^2 + \ldots + f(x_k) \cdot n^{k-1} \ .$$

Zamiana ciągu liter na liczbę

Jak zamienić ciąg liter długości k na liczbę naturalną?
Odwrotnie, jak zamienić liczbę naturalną na ciąg liter?

Niech X będzie pewnym alfabetem (zbiorem liter).
Załóżmy, że $|X| = n$. Każdej literze przyporządkujemy odpowiednik liczbowy ze zbioru $\{0, 1, \ldots, n-1\}$. Oznaczmy to przyporządkowanie poprzez f.

Mamy słowo $u = x_1 x_2 \ldots x_k$, gdzie $x_i \in X$ dla $1 \leqslant i \leqslant k$. Wtedy

$$u \longleftrightarrow f(x_1) + f(x_2) \cdot n + f(x_3) \cdot n^2 + \ldots + f(x_k) \cdot n^{k-1} \ .$$

Otrzymujemy liczbę ze zbioru $\{0, 1, 2, \ldots, n^k - 1\}$.

Przykład

Alfabet $X = \{\text{A,Ą,B,C,Ć,}\ldots\text{,Z,Ź,Ż}\}$

Zamieniamy słowo $u = \text{KOT}$ na liczbę ze zbioru $\{0, 1, \ldots, 32767\}$ $(32^3 - 1 = 32767)$.

$$f(\text{K}) = 13,\ f(\text{O}) = 19,\ f(\text{T}) = 25$$

$$\text{KOT} \longleftrightarrow 13 + 19 * 32 + 25 * 32^2 = 26221$$

Przykład

Zamienimy liczbę $m = 19053$ na ciąg liter długości 3.

Przykład

Zamienimy liczbę $m = 19053$ na ciąg liter długości 3.

Dzielenie m przez 32 z resztą:

$m = 595 \cdot 32 + 13$

Przykład

Zamienimy liczbę $m = 19053$ na ciąg liter długości 3.

Dzielenie m przez 32 z resztą:

$m = 595 \cdot 32 + 13 \longrightarrow 13 = f(\mathrm{K})$

Przykład

Zamienimy liczbę $m = 19053$ na ciąg liter długości 3.

Dzielenie m przez 32 z resztą:

$m = 595 \cdot 32 + 13 \longrightarrow 13 = f(\mathrm{K})$

$m_1 = (m - 13)/32 = 595$

Przykład

Zamienimy liczbę $m = 19053$ na ciąg liter długości 3.

Dzielenie m przez 32 z resztą:

$$m = 595 \cdot 32 + 13 \longrightarrow 13 = f(\mathrm{K})$$

$$m_1 = (m - 13)/32 = 595$$

$$m_1 = 18 \cdot 32 + 19$$

Przykład

Zamienimy liczbę $m = 19053$ na ciąg liter długości 3.

Dzielenie m przez 32 z resztą:

$$m = 595 \cdot 32 + 13 \longrightarrow 13 = f(\mathrm{K})$$

$$m_1 = (m - 13)/32 = 595$$

$$m_1 = 18 \cdot 32 + 19 \longrightarrow 19 = f(\mathrm{O})$$

Przykład

Zamienimy liczbę $m = 19053$ na ciąg liter długości 3.

Dzielenie m przez 32 z resztą:

$$m = 595 \cdot 32 + 13 \longrightarrow 13 = f(\mathrm{K})$$

$$m_1 = (m - 13)/32 = 595$$

$$m_1 = 18 \cdot 32 + 19 \longrightarrow 19 = f(\mathrm{O})$$

$$m_2 = (m_1 - 19)/32 = 18$$

Przykład

Zamienimy liczbę $m = 19053$ na ciąg liter długości 3.

Dzielenie m przez 32 z resztą:

$$m = 595 \cdot 32 + 13 \longrightarrow 13 = f(\mathrm{K})$$

$$m_1 = (m - 13)/32 = 595$$

$$m_1 = 18 \cdot 32 + 19 \longrightarrow 19 = f(\mathrm{O})$$

$$m_2 = (m_1 - 19)/32 = 18$$

$$m_2 = 0 \cdot 32 + 18$$

Przykład

Zamienimy liczbę $m = 19053$ na ciąg liter długości 3.

Dzielenie m przez 32 z resztą:

$m = 595 \cdot 32 + 13 \longrightarrow 13 = f(\mathrm{K})$

$m_1 = (m - 13)/32 = 595$

$m_1 = 18 \cdot 32 + 19 \longrightarrow 19 = f(\mathrm{O})$

$m_2 = (m_1 - 19)/32 = 18$

$m_2 = 0 \cdot 32 + 18 \longrightarrow 18 = f(\acute{\mathrm{N}})$

Otrzymaliśmy słowo: KOŃ

Kryptosystemy z kluczem publicznym

Osoba A tworzy poufnie dwa klucze (matematycznie powiązane). Jeden z nich nazywany jest **kluczem publicznym**, a drugi **kluczem prywatnym**. Obliczenie klucza prywatnego na podstawie klucza publicznego jest praktycznie niewykonalne. Klucz publiczny może być swobodnie rozpowszechniany, natomiast odpowiadający mu klucz prywatny musi zostać zachowany w sekrecie.

Osoba B chcąc wysłać do A wiadomość używa do jej zaszyfrowania klucza publicznego.

Osoba A otrzymany od B szyfrogram odszyfrowuje przy użyciu klucza tajnego.

Kryptosystemy z kluczem publicznym

Osoba A tworzy poufnie dwa klucze (matematycznie powiązane). Jeden z nich nazywany jest **kluczem publicznym**, a drugi **kluczem prywatnym**. Obliczenie klucza prywatnego na podstawie klucza publicznego jest praktycznie niewykonalne. Klucz publiczny może być swobodnie rozpowszechniany, natomiast odpowiadający mu klucz prywatny musi zostać zachowany w sekrecie.

Osoba B chcąc wysłać do A wiadomość używa do jej zaszyfrowania klucza publicznego.

Osoba A otrzymany od B szyfrogram odszyfrowuje przy użyciu klucza tajnego.

Zaleta: Osoby A i B nie muszą się spotykać w celu ustalenia kluczy.

Kryptosystem RSA

Został stworzony w 1978 przez zespół: Ronald Rivest, Adi Shamir, Leonard Adleman.

Kryptosystem RSA

Został stworzony w 1978 przez zespół: Ronald Rivest, Adi Shamir, Leonard Adleman.

Osoba A - konstrukcja kluczy:

- losuje dwie duże liczby pierwsze p i q,
- losuje liczbę e taką, że

$$1 < e < (p-1)(q-1) \quad \text{i} \quad NWD(e,(p-1)(q-1)) = 1 \ ,$$

- oblicza $n = p \cdot q$
- oblicza $d = e^{-1} \pmod{(p-1)(q-1)}$

Klucz publiczny: (n, e)

Klucz prywatny: (n, d)

Szyfrowanie: Osoba B chce wysłać wiadomość do osoby A. Oblicza reprezetację liczbową m swojej wiadomości. Wykorzystując klucz publiczny oblicza

$$c = m^e \pmod{n} .$$

Deszyfrowanie: Osoba A oblicza

$$c^d \pmod{n} = m .$$

Dzielenie tajemnicy

Podział tajemnicy pomiędzy trzy osoby, tak aby do odtworzenia jej były potrzebne co najmniej dwie z nich.

Dzielenie tajemnicy

Podział tajemnicy pomiędzy trzy osoby, tak aby do odtworzenia jej były potrzebne co najmniej dwie z nich.

Załóżmy, że tajną informacją jest liczba N.

Dzielenie tajemnicy

Podział tajemnicy pomiędzy trzy osoby, tak aby do odtworzenia jej były potrzebne co najmniej dwie z nich.

Załóżmy, że tajną informacją jest liczba N.

Podział tajemnicy: Wybieramy na płaszczyźnie pewien punkt $P = (N, y)$. Przeprowadzamy przez niego trzy różne proste. Równania prostych przekazujemy trzem osobom, tak aby każda z nich znała tylko jedno.

Dzielenie tajemnicy

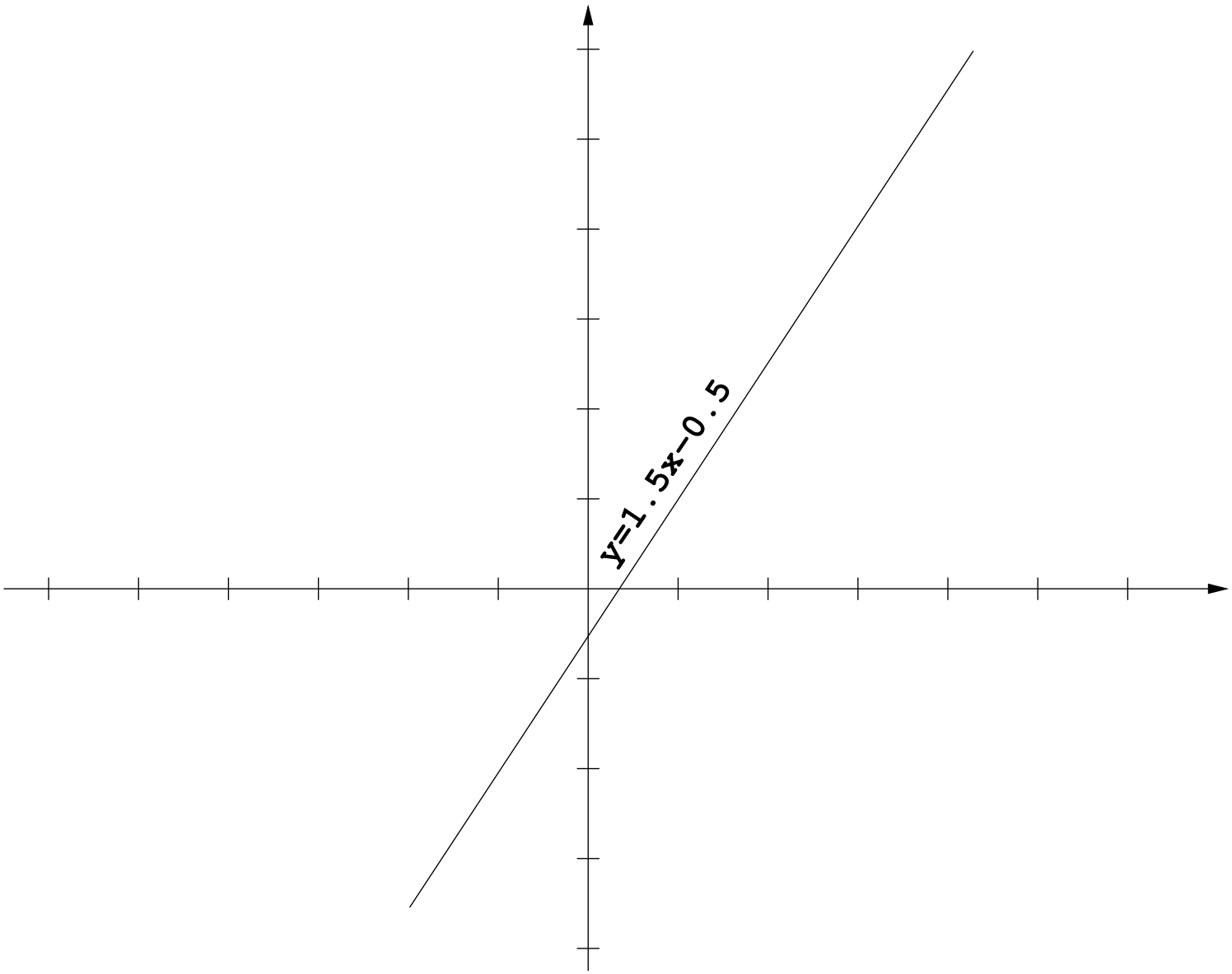
Podział tajemnicy pomiędzy trzy osoby, tak aby do odtworzenia jej były potrzebne co najmniej dwie z nich.

Załóżmy, że tajną informacją jest liczba N.

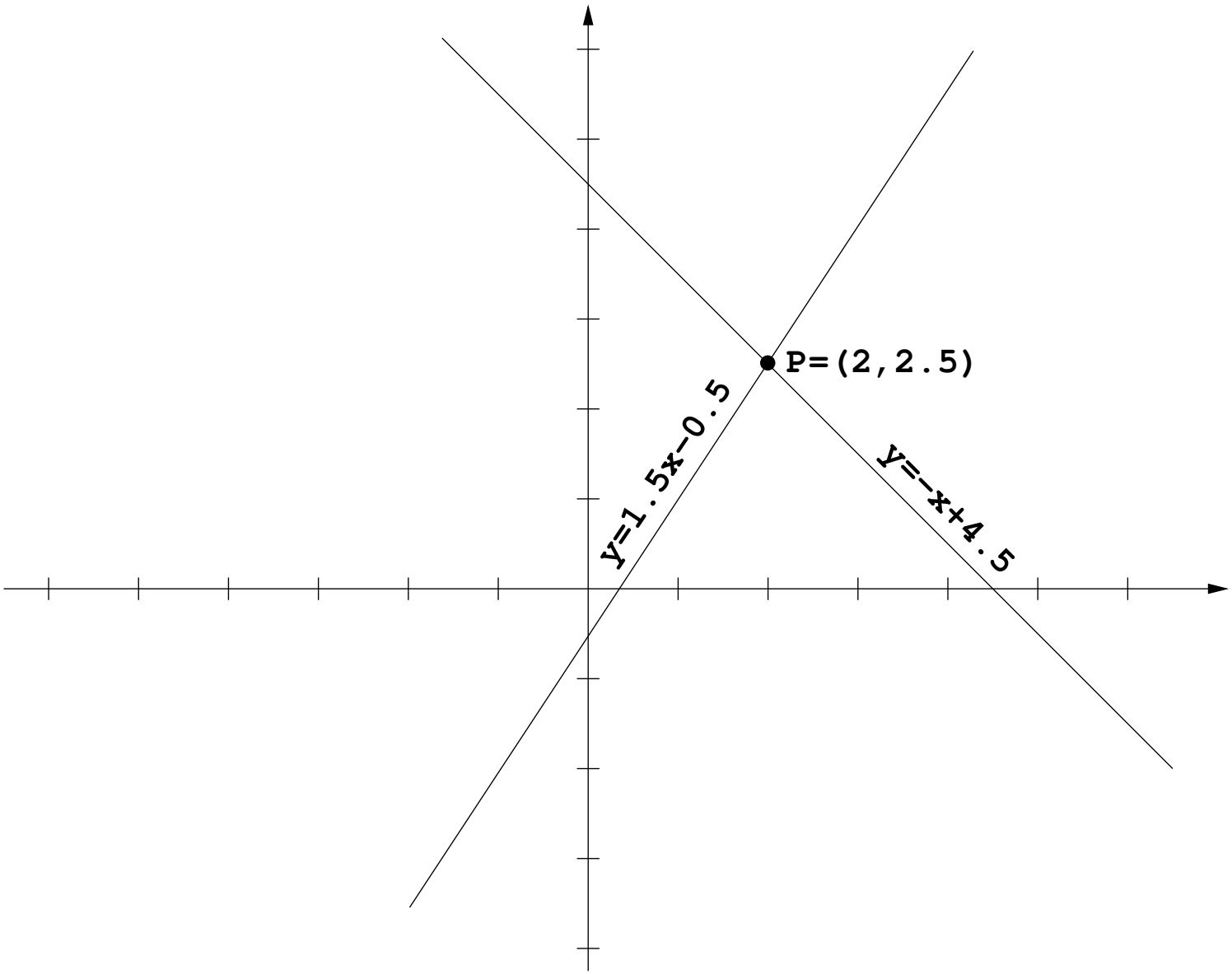
Podział tajemnicy: Wybieramy na płaszczyźnie pewien punkt $P = (N, y)$. Przeprowadzamy przez niego trzy różne proste. Równania prostych przekazujemy trzem osobom, tak aby każda z nich znała tylko jedno.

Odtworzenie tajemnicy: Dowolne dwie osoby rozwiązują układ równań składający się z równań prostych jakie one znają. Rozwiązaniem tego układu jest punkt przecięcia tych prostych P. Osoby odczytują pierwszą współrzedną tego punktu.

Dzielenie tajemnicy - jedna osoba



Dzielenie tajemnicy - dwoje osób



Problem logarytmu dyskretnego

Niech p będzie dużą liczbą pierwszą.

Przyjmujemy oznaczenie:

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} \ .$$

Problem logarytmu dyskretnego

Niech p będzie dużą liczbą pierwszą.

Przyjmujemy oznaczenie:

$$\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\} \ .$$

Ustalmy $g \in \mathbb{Z}_p^*$.

Problemem logarytmu dyskretnego w $\mathbb{Z}_p^*$ przy podstawie g nazywamy zadanie wyznaczenia dla danego $y \in \mathbb{Z}_p^*$ takiej liczby naturalnej n, że $y = g^n \pmod{p}$ (o ile takie n istnieje).

System wymiany kluczy Diffego-Hellmana

Zadanie: Osoby A i B chcą uzgodnić wspólny klucz (klucze), którego będą używały do szyfrowania metodami klasycznymi. Jednocześnie, osoby te nie mogą się ze sobą spotkać ze względu na dzielące ich odległości zamieszkania.

System wymiany kluczy Diffego-Hellmana

Zadanie: Osoby A i B chcą uzgodnić wspólny klucz (klucze), którego będą używały do szyfrowania metodami klasycznymi. Jednocześnie, osoby te nie mogą się ze sobą spotkać ze względu na dzielące ich odległości zamieszkania.

1. Kanałem nieszyfowanym osoby A i B uzgadniają dużą liczbę pierwszą p oraz pewien element $g \in \mathbb{Z}_p^*$.

System wymiany kluczy Diffego-Hellmana

Zadanie: Osoby A i B chcą uzgodnić wspólny klucz (klucze), którego będą używały do szyfrowania metodami klasycznymi. Jednocześnie, osoby te nie mogą się ze sobą spotkać ze względu na dzielące ich odległości zamieszkania.

1. Kanałem nieszyfowanym osoby A i B uzgadniają dużą liczbę pierwszą p oraz pewien element $g \in \mathbb{Z}_p^*$.

2. Osoba A w tajemnicy wybiera losową liczbę $k_A < p$ i oblicza resztę z dzielenia g^{k_A} przez p i wynik wysyła osobie B.

System wymiany kluczy Diffego-Hellmana

Zadanie: Osoby A i B chcą uzgodnić wspólny klucz (klucze), którego będą używały do szyfrowania metodami klasycznymi. Jednocześnie, osoby te nie mogą się ze sobą spotkać ze względu na dzielące ich odległości zamieszkania.

1. Kanałem nieszyfowanym osoby A i B uzgadniają dużą liczbę pierwszą p oraz pewien element $g \in \mathbb{Z}_p^*$.

2. Osoba A w tajemnicy wybiera losową liczbę $k_A < p$ i oblicza resztę z dzielenia g^{k_A} przez p i wynik wysyła osobie B.

3. Osoba B robi podobnie: wysyła do osoby A resztę $g^{k_B} \pmod{p}$, utrzymując $k_B < p$ w tajemnicy.

System wymiany kluczy Diffego-Hellmana

Zadanie: Osoby A i B chcą uzgodnić wspólny klucz (klucze), którego będą używały do szyfrowania metodami klasycznymi. Jednocześnie, osoby te nie mogą się ze sobą spotkać ze względu na dzielące ich odległości zamieszkania.

1. Kanałem nieszyfowanym osoby A i B uzgadniają dużą liczbę pierwszą p oraz pewien element $g \in \mathbb{Z}_p^*$.

2. Osoba A w tajemnicy wybiera losową liczbę $k_A < p$ i oblicza resztę z dzielenia g^{k_A} przez p i wynik wysyła osobie B.

3. Osoba B robi podobnie: wysyła do osoby A resztę $g^{k_B} \pmod p$, utrzymując $k_B < p$ w tajemnicy.

4. Uzgodnionym kluczem będzie:

$$g^{k_A k_B} \pmod p = (g^{k_A})^{k_B} \pmod p = (g^{k_B})^{k_A} \pmod p .$$

Funkcje skrótu

Funkcja skrótu (funkcja haszująca) jest to funkcja, która przyporządkowuje dowolnie dużej wiadomości krótką, posiadającą stały rozmiar wartość (skrót wiadomości).

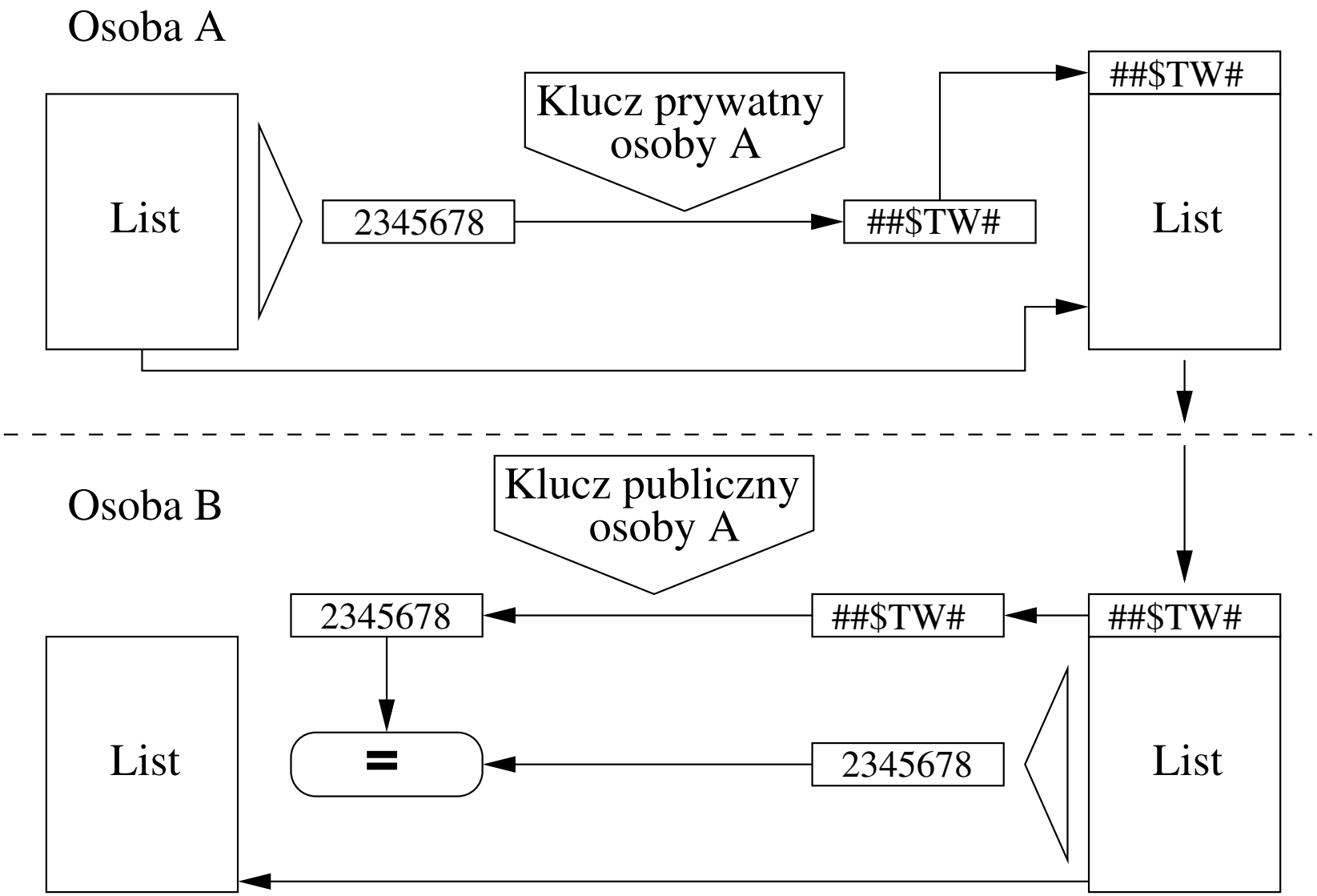
Funkcja skrótu $H(m)$ musi posiadać własności:

1) dla każdej wiadomości m łatwo jest obliczyć $H(m)$;

2) praktycznie niemożliwe jest znalezienie takich dwóch wiadomości m i m', dla których $H(m) = H(m')$ (tzw. odporność na kolizje);

3) dla danego skrótu y praktycznie nie można znaleźć takiego m, że $H(m) = y$ (odporność na wyliczenie przeciwobrazu).

Podpis cyfrowy



Bibliografia

- Neal Koblitz, *Wykład z teorii liczb i kryptografii,* WNT, Warszawa 2006
- Neal Koblitz, *Algebraiczne aspekty kryptografii,* WNT, Warszawa 2000
- Alfred Menezes, Paul van Oorschot, *Kryptografia stosowana,* WNT, Warszawa 2005

A. Menezes, P. van Oorschot - Handbook of applied cryptography

http://www.cacr.math.uwaterloo.ca/hac/

Dziękuję za uwagę.

KONIEC