

# Kryptografia

## Rozdzielanie tajemnicy

**dr Robert Borowiec**

Politechnika Wrocławska

Instytut Telekomunikacji i Akustyki

pokój 908, C-5

tel. 3203083

e-mail: [robert.borowiec@ita.pwr.wroc.pl](mailto:robert.borowiec@ita.pwr.wroc.pl)

www: [lstwww.ita.pwr.wroc.pl/~RB/](http://lstwww.ita.pwr.wroc.pl/~RB/)

**Wykład XII**

**30-minut**

## Dzielenie wiadomości pomiędzy grupę osób

- Protokół dzielenia informacji pomiędzy grupę  $N$  osób jest następujący:
- Arbiter generuje  $N-1$  losowych kluczy:  $k_1, k_2, \dots, k_{N-1}$  o tej samej długości co wiadomość  $M$ .
- Arbiter oblicza sumę modulo 2 wszystkich kluczy i dzielonej wiadomości w wyniku czego wyznacza kryptogram  $C$
- $k_1 \oplus k_2 \oplus \dots \oplus k_{N-1} \oplus M = C$
- Rozdziela pomiędzy osoby klucze  $k_i$  oraz szyfrogram  $C$ .
- Wyznaczenie wiadomości jawnej jest możliwe po zsumowaniu wszystkich kluczy i kryptogramu

# Dzielenie wiadomości

- Wady i zalety dzielenia tajemnicy
  - ⇒ tajemnica nie może być ujawniona bez zgody wszystkich zaangażowanych w nią osób;
  - ⇒ utrata choćby jednego klucza uniemożliwia odtworzenie informacji jawnej;
  - ⇒ gdy w grupie osób jest oszust, to nie można go wykryć, ani odczytać informacji;
  - ⇒ ujawnienie wiadomości zależy od woli poszczególnych powierników tajemnicy. Każdy z nich może skutecznie zablokować odzyskanie informacji jawnej



# Progowo dzielenie tajemnicy

- W systemach z progowym podziałem tajemnicy wystarczy, że tylko  $n$  kluczy z ogólnej liczby  $m$  zostanie ujawnionych. Metoda opiera się na algorytmie wielomianu interpolacyjnego Lagrange'a.
- Idea metody:

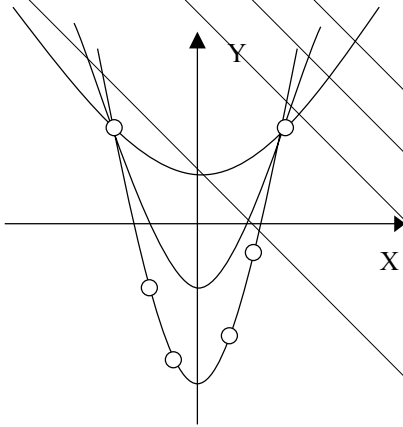
Jeżeli dana jest funkcja w postaci wielomianu stopnia  $m-1$

$$f(x) = v_{m-1} \cdot x^{m-1} + v_{m-2} \cdot x^{m-2} + \dots + v_0$$

to możemy jednoznacznie wyznaczyć współczynniki wielomianu  $v_i$ , jeżeli będziemy znali wartość funkcji  $f(x)$  w  $m$  punktach  $x_i$ . Wobec tego będzie możliwe ułożenie i rozwiązanie układu  $m$  równań liniowych.



## Przykład wielomianu



Przez dwa dowolne punkty na płaszczyźnie możemy poprowadzić nieskończenie wiele funkcji parabolicznych

$$f(x) = ax^2 + bx + c$$

Przy danych trzech punktach możliwe jest poprowadzenie już tylko jednej paraboli.

Do jednoznacznego wyznaczenia współczynników  $a, b, c$  w równaniu paraboli konieczna jest więc znajomość co najmniej trzech dowolnych punktów z  $n$  leżących na paraboli.



## Schemat progowy współdzielenia tajemnicy

- W Wiadomość poufna jest dzielona na  $n$  części (cienie), tak aby  $m$  dowolnie wybranych cieni umożliwiała odtworzenie utajnionej treści.
- Schemat protokołu:
  - ⇒ Wybierana jest liczba pierwsza  $p$ , większa od liczby możliwych cieni oraz reprezentacji liczbowej informacji jawnej;
  - ⇒ W celu dzielenia tajemnicy generowany jest wielomian stopnia  $m-1$ , gdzie  $m$  oznacza niezbędny próg ilości znanych kluczy;
  - ⇒ Cienie uzyskuje się przez obliczenie wartości wielomianu  $k_i = f(x_i)$ , w  $n$  różnych punktach  $x_i = 1, 2, \dots, n$ ;
  - ⇒ Ujawnia się wartości cieni oraz  $k_i$  oraz znane są  $x_i$



## Schemat progowy współdzielenia tajemnicy

- Zalety i wady
  - ⇒ tajemnica nie może być ujawniona bez zgody wymaganej ilości osób;
  - ⇒ utrata nawet części kluczy, jeżeli zachowana została ich wymagana ilość, nie blokuje odtworzenia informacji jawnej;
  - ⇒ ujawnienie wiadomości zależy od woli grupy, a nie pojedynczej osoby;
  - ⇒ w systemie progowym  $(m, n)$  można wykryć  $k$  oszukujących, jeżeli dysponujemy  $m+k$  kluczami, przy założeniu, że  $m+k \leq n$ .



## Protokoły pośrednie i kanał podprogowy

- Protokół przekazania informacji podprogowej ukrytej w podpisie cyfrowym
- Alicja wybiera nie budzącą podejrzeń jawna wiadomość.
- Kluczem tajnym współdzielonym z Robertem podpisuje wiadomość ukrywając informacje podprogowe w podpisie.
- Alicja wysyła całą informację przez strażnika do Roberta.
- Robert po otrz
- Przy użyciu klucza tajnego, współdzielonego z Bobem
- Schemat protokołu:
  - ⇒ Wybierana jest liczba pierwsza  $p$ , większa od liczby możliwych cieni oraz reprezentacji liczbowej dzielonej tajemnicy;
  - ⇒ W celu dzielenia tajemnicy generowany jest wielomian stopnia  $m-1$ .
  - ⇒ Cienie uzyskuje się przez obliczenie wartości wielomianu w różnych punktach  $k_i = F(k_i)$ .

A series of parallel diagonal lines crossing the slide from the top-left to the bottom-right.

KONIEC

Dziękuję za uwagę