

# Kryptografia

## Jednokierunkowe funkcje skrótu

**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)

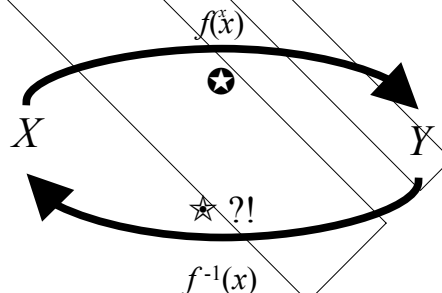
www: [lstwww.ita.pwr.wroc.pl/~RB/](http://lstwww.ita.pwr.wroc.pl/~RB/)

**Wykład X**

**15-minut**

## Funkcja jednokierunkowa

- **Funkcja jednokierunkowa**  $f(x)$  jest to funkcja, dla której łatwo policzyć  $y=f(x)$  dla znanego argumentu  $x$ . Jednak znając wartość funkcji  $y$ , trudno jest wyznaczyć argument  $x=f^{-1}(y)$ .



## Jednokierunkowa funkcja skrótu

- *Jednokierunkowa funkcja skrótu* jest to funkcja jednokierunkowa, która w wyniku daje wartość o konkretnej ustalonej długości.
- Właściwości funkcji skrótu:
  - ⇒ dla zadanej wiadomości  $M$  funkcja umożliwia łatwe wyznaczenie  $f(M)$ ;
  - ⇒ dla zadanej wartości  $y$  trudno jest wyznaczyć wiadomość  $M=f^{-1}(y)$ ;
  - ⇒ dla zadanej wiadomości  $M$  trudno jest wyznaczyć inną wiadomość  $M'$  dla której funkcja  $f$  wytwarza taki sam skrót  $f(M)=f(M')$ ;



## Kryptoanaliza funkcji skrótu

- *Funkcja skrótu powinna spełniać trzy warunki:*
  - ⇒ *Nieemożliwe jest odtworzenie wiadomości  $M$  (wartości argumentu funkcji) znając wynik funkcji;*
  - ⇒ *Musi być trudno obliczeniowo znaleźć wiadomość  $M'$ , która w wyniku da tą samą wartość skrótu jak wiadomość  $M$ ;*
  - ⇒ *Musi być trudno obliczeniowo znaleźć takie dwie losowe wiadomości  $M$  i  $M'$  dające po skróceniu samą wartość (atak metoda dnia urodzin). Żaden atak nie powinien być bardziej efektywny niż metoda brutalna;*



# Kryptoanaliza funkcji skrótu

## ➤ *Paradoks dnia urodzin:*

- ⇒ *Ile osób musi liczyć grupa, aby była znaczna szansa na to aby, ktoś z tej grupy miał urodziny określonego dnia.*
  - » Odpowiedź 183 osoby<sup>x</sup>
- ⇒ *Ile osób musi liczyć grupa, aby była znaczna szansa na to, aby znalazły się w niej dwie osoby o tej samej dacie urodzin.*
  - » Odpowiedź 23 osoby, co daje 253 możliwe pary



# Kryptoanaliza funkcji skrótu

- *Przy funkcji skrótu, która skraca wiadomość  $M$  do słowa o długości  $h$  bitów znalezienie wiadomości  $M'$ , która skraca się do takiej samej wartości jak wiadomość  $M$  wymaga wykonania sprawdzenia  $2^h$  losowo wybranych wiadomości.*
  - <sup>x</sup>
- *Znalezienie dwóch dowolnych wiadomości  $M$  i  $M'$  skracających się do tej samej wartości o długości  $h$  bitów wymaga sprawdzenia  $2^{h/2}$  losowo wybranych wiadomości.*



## Znane funkcje skrótu

- *Snerfu*
- *N-hash*
- *MD2*
- *MD4*
- *MD5*
- *Ripe-MD*
- *HAVAL*
- *SHA*



## Funkcja SHA

- *SHA ( ang. Secure Hash Algorithm) jest standardem w Stanach Zjednoczonych*
- *Cechy SHA:*
  - ⇒ *wytwarza skrót o długości 160 bitów;*
  - ⇒ *przeznaczony jest do skracania wiadomości o długości mniejszej niż  $2^{64}$  bitów, ale większej od 0.*



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

# KONIEC

## Dziękuję za uwagę