22 aprilie 2019

# Seminarul nr. 1 - Criptografie

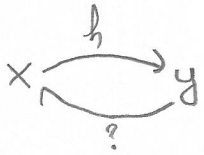
## ■ Funcții hash

hash $h: X \to Z$, $|X| > |Z|$

$h: \{0,1\}^t \to \{0,1\}^l$, $t > l$

$h: \{0,1\}^* \to \{0,1\}^l$

Proprietăți:




- **one-way**: ușor de evaluat, greu de inversat
  $\forall y \in Z$ (Im(h)), este dificil de găsit $x \in X$ a.î. $h(x) = y$

Pt. a dem. că nu e one-way

- **slab rezistentă la coliziuni** dată $\forall x \in X$, este dificil de a găsi $x' \neq x$ a.î. $h(x') = h(x)$ (h, x / x')
- **tare rezistentă la coliziuni** dacă este dificil de a genera 2 elemente $x, x' \in X$, $x \neq x'$ a.î. $h(x) = h(x')$ (h / x, x')

## ■ Exerciții

(6p) 1. Definim $h: \bigcup_{\substack{160 \mid m \\ m \neq 0}} \{0,1\}^m \longrightarrow \{0,1\}^{160}$ astfel

Input $x$ $\quad x = x_1 \dots x_k$, $|x_i| = 160$

$h(x) = neg(x_1) \oplus neg(x_2) \oplus \dots \oplus neg(x_k)$

a) h este one-way? (2p)
b) h slab rezistentă? (2p) Justificare
c) h tare rezistentă? (2p)

(2p) 2. Fie $g: \{0,1\}^* \to \{0,1\}^t$, g tare rezistentă. Definim $h: \{0,1\}^* \to \{0,1\}^{t+1}$

$$h(x) = \begin{cases} 1x, \text{ dacă } |x| = t \\ 0g(x), \text{ altfel} \end{cases}$$

Demonstrați că h este tare rezistentă la coliziuni. (Hint: RA)

(6p) 3. Fie $h: \{0,1\}^{t+1} \to \{0,1\}^t$ tare rezistentă.

Construim $\overline{h}: \bigcup_{i \geq t+1} \{0,1\}^i \to \{0,1\}^t$ astfel:

Input: $x \in \bigcup_{i \geq t+1} \{0,1\}^i$

Output: $\overline{h}(x)$

begin

construiește $y(x) = 11 f(x)$, $f$ homomorfism (aplică bit cu bit)

$f: \{0,1\}^* \to \{0,1\}^*$, $f(0) = 0$

$f(1) = 01$

$y(x) = x_1 x_2 \dots x_k$, $x_i \in \{0,1\}$

$g_0 = 0^t$

for $i = 1$ to $k$ do

$g_i = h(g_{i-1} x_i)$

return $(g_k)$

end

Demonstrați că $\overline{h}$ e tare rezistentă. (Hint: Dem că $\forall x \neq x'$, $y(x)$ nu e sufix $\sin y(x')$)

~~Rezolvare~~ Ciornă

1.

$$\begin{array}{r} 111111 \oplus \\ 001100 \\ \hline 110011 \end{array} \qquad \begin{array}{r} 001100 \oplus \\ 110011 \\ \hline 111111 \end{array}$$

$0 \to 0$

$1 \to 01$

Rezolvare

1. a) Fie $y \in \{0,1\}^{160}$ oarecare.

$\Rightarrow \exists\, x \in \{0,1\}^{160} \subset X$ aî $x = neg(y)$

$x = x_1 \dots x_k$, $|x_i| = 160$

$|x| = 160 \Rightarrow k = 1$

deci $h(x) = neg(x_1) \oplus neg(x_2) \oplus \dots \oplus neg(x_k) =$

$= neg(x_1) = neg(x) = neg(neg(y)) = y$

Deci $\forall y \in Z$, se găsește $x = neg(y) \in \{0,1\}^{160}$ aî $h(x) = y$

$\rightarrow$ h nu e one-way

b) I. $x \in \{0,1\}^{160}$

$\exists\, x' = x_1 x_2 x_3 \in \{0,1\}^{160 \cdot 3}$ astfel încât $x_1 = neg(x_3)$, $x_1 \in \{0,1\}^{160}$

și $x_2 = h(x) = y$

$h(x') = neg(x_1) \oplus neg(x_2) \oplus neg(x_3) =$

$= x_3 \oplus neg(x_2) \oplus neg(x_3) =$

$= x_3 \oplus neg(x_3) \oplus neg(x_2) =$ ($\oplus$ e comutativ) $a \oplus b = b \oplus a$)

$= 1^{160} \oplus neg(x_2) =$

$= x_2 = h(x)$

II. $x = x_1 x_2 \dots x_k$, $|x_i| = 160$, $k > 1$

$\rightarrow \exists\, x' = x_k x_2 \dots x_{k-1} x_1$

$h(x) = neg(x_1) \oplus neg(x_2) \oplus \dots \oplus neg(x_k)$

$h(x') = (neg(x_k) \oplus neg(x_2) \oplus \dots \oplus neg(x_{k-1}) \oplus neg(x_1) =$

$= neg(x_1) \oplus neg(x_k) \oplus neg(x_2) \oplus \dots \oplus neg(x_{k-1}) =$

$= neg(x_1) \oplus neg(x_2) \oplus \dots \oplus neg(x_k) = h(x)$

I, II $\Rightarrow$ h nu e slab rezistentă

c)

2. $P_p$ RA $h$ nu e tare nr existentă la coliziuni

$\Rightarrow$ Este unor de găsit $x, x' \in X$, $x \neq x'$ a.î. $h(x) = h(x')$

I $|x| = t \to h(x) = 1x$
$|x'| = t \to h(x') = 1x'$
$\Rightarrow h(x) = h(x')$
$\to 1x = 1x' \to x = x'$ Contradicție

II $|x| = t \Rightarrow h(x) = 1x$
$|x'| \neq t \Rightarrow h(x') = og(x')$
$h(x) = h(x')$
$\to 1x = og(x')$ Fals

III $|x| \neq t$, $|x'| = t$ cazul simetric al lui II
analog $\to 1x' = og(x)$ Fals

IV $|x| \neq t \Rightarrow h(x) = og(x)$
$|x'| \neq t \Rightarrow h(x') = og(x')$
$h(x) = h(x')$
$\to og(x) = og(x')$

$\to g(x) = g(x')$

$\to$ se pot găsi unor $x, x' \in X$, $x \neq x'$ a.î. $g(x) = g(x') \to g$ nu e tare nr existentă

Contradicție cu ipoteza

I, II, III, IV $\Rightarrow$ pp falsă, deci $h$ e tare nr existentă

3. Fie $x, x' \in \bigcup_{i \geq t+1} \{0,1\}^i$

$x = a_1 a_2 \dots a_k \quad k, \ell \geq t+1$

$x' = b_1 b_2 \dots b_\ell \quad x_i, x'_i \in \{0,1\}$

~~$x \neq x' \Rightarrow \exists i \in \{1, \dots \min(k,\ell)\}$ a.î. $a_i \neq b'_i$~~ ($\min(k,\ell) = k$)

~~$x \neq x'$ a.î. $h(x) = h(x')$~~

~~$f(x) = d_1 d_2 \dots d_k$, $k < \ell$~~

~~$f(x') = e_1 e_2 \dots e_\ell$~~

fie $i \in \{1, \dots k-1\}$ a.î. $d_{k-j} = b_{\ell-j}$, $\forall j \in \overline{0, i-1}$

$a_{k-i} \neq b_{\ell-i}$

- $a_{k-i} = 0 \rightarrow f(a_{k-i}) = 0$
  $b_{\ell-i} = 1 \Rightarrow f(b_{\ell-i}) = 01$

  $f(x)$ nu va mai fi sufix pentru $f(x')$, deoarece următorul bit generat de $f(a_{k-i+1})$ va fi $0 \neq 1$ iar $f(x')$ nu va fi sufix pentru $f(x)$, ~~deoarece~~

- $a_{k-i} = 1$ cazul este simetric
  $b_{\ell-i} = 0$

Deci, pornind de la dreapta la stânga, primul bit care va diferi va duce la generarea unor sufixe diferite.

$\rightarrow \forall x \neq x'$, $f(x)$ nu e sufix pentru $f(x') \rightarrow$ ~~$f(x)$ nu e sufix~~

---

M nu poate fi sufix pentru $f(x)$, construcția nu permite să se întâmple asta deoarece dacă $y(x)$ sufix al lui $y(x') \Rightarrow$ NU sufix

Pp RA $\bar{h}$ nu e tare rezistentă $\Rightarrow$ e uşor de găsit $x, x' \in \bigcup_{i \geq t+1} \{0,1\}^i$ $g x \neq x'$ a.î. $\bar{h}(x) = \bar{h}(x')$

Fără a pierde din generalitate, presupunem că $|y(x)| \leq |y(x')|$

~~Fie $k = \min\{|y(x)|, |y(x')|\}$~~

~~$\bar{h}(x) = \bar{h}(x') \Leftrightarrow h(g_{k-1}) = h(g_{k-1})$~~

Fie $k = |y(x)|$

$\ell = |y(x')|$

$\bar{h}(x) = \bar{h}(x') \Leftrightarrow h(g_{k-1} x_k) = h(g_{\ell-1} x_\ell)$ $\Rightarrow g_{k-1} x_k = g_{\ell-1} x_\ell \rightarrow \begin{cases} x_k = x_\ell \\ g_{k-1} = g_{\ell-1} \end{cases}$

perechea $(x, x')$ e uşor de găsit

$h$ tare rezistentă

$g_{k-1} = g_{\ell-1} \Rightarrow h(g_{k-2} x_{k-1}) = h(g_{\ell-2} x_{\ell-1})$ $\Rightarrow g_{k-2} x_{k-1} = g_{\ell-2} x_{\ell-1} \rightarrow \begin{cases} x_{k-1} = x_{\ell-1} \\ g_{k-2} = g_{\ell-2} \end{cases}$

perechea $(x, x')$ uşor de găsit

$h$ tare rezistentă

$\vdots$

$g_1 = g_{\ell-k-1} \Rightarrow h(g_0 x_1) = h(g_{\ell-k-2} x_{\ell-k-1})$ $\rightarrow g_0 x_1 = g_{\ell-k-2} x_{\ell-k-1}$

perechea $(x, x')$ uşor de găsit

$h$ tare rezistă $\rightarrow x_1 = x_{\ell-k-1}$

$x_k = x_\ell$

$x_{k-1} = x_{\ell-1}$ $\rightarrow$ $f(x)$ sufix în $f(x')$ - $g(x)$ sufix în $g(x')$

contradicţie

$\vdots$

$x_1 = x_{\ell-k-1}$

$\rightarrow$ pp falsă e falsă $\rightarrow$ $\bar{h}$ e tare rezistentă