Szyfry strumieniowe II (INTEGRITY)

Nowy problem: **MALLEABILITY**

modyfikacja kryptogramu wpływa w przewidywalny sposób na tekst jawny

Alicja

$m =$ Eve

$c = (IV,\ m \oplus G(IV, k))$

Bank

Bob

dec

$c \oplus x$

Adv

$x \leftarrow (0^{|}, y)$

Message Authentication Codes (MAC)

(Gen, Mac, Vrfy)

Digital Signatures

(Gen, Sign, Vrfy)

$(pubK, privK) \leftarrow Gen(1^n)$ $\quad$ $k \leftarrow Gen(1^n)$

$s \leftarrow Sign(privK, m)$ $\quad$ $t \leftarrow Mac(k, m)$

$b = Vrfy(pubK, m, s)$ $\quad$ $b = Vrfy(k, m, t)$

$\uparrow$ $\quad$ $\uparrow$

$\{0,1\}$ $\quad$ $\{0,1\}$

Alicja

.....to: Eve....

$Enc(k,m)$ $Mac(k,c)$

(c, t)

Adv

$c' = f(c, \dots)$

$t' = f(c, t, \dots)$

Bank

(c', t')

if $Vrfy(k, c', t') == 1$:

$m' = Dec(k, c')$

else:

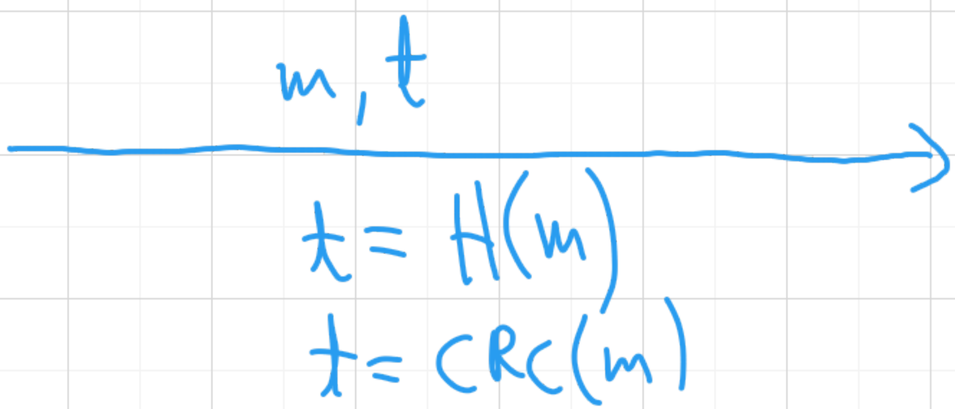
problem

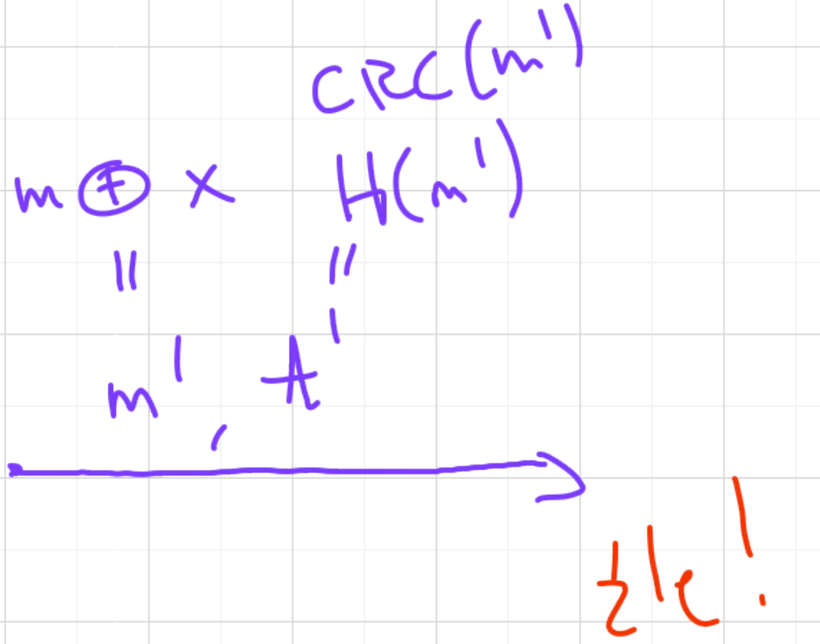
jakie własności powinien mieć dobry schemat MAC?

Przykład 1 (brak klucza)

MAC = CRC

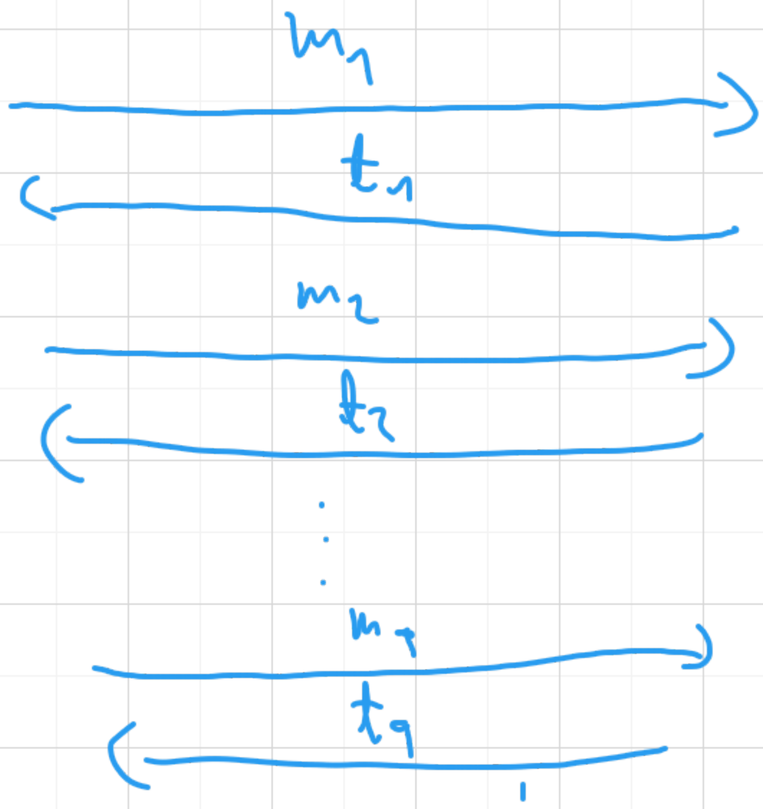
MAC = h





Niepodrabialność (Unforgestibility) MAC

Adv



Oracle (k)

$m \notin \{m_1, \dots, m_q\}$

$P[Vrfy(k, m, t) = 1]$ - negligible

$P[Vrfy(pubk, m, s) = 1]$

prawdopodobieństwo $< \frac{1}{2^{80}}$

to Adv nie powinien móc wygenerować poprawnego tagu pod kątem wiadomości dla podpisu

Wykorzystywane w praktyce:

CBC-MAC — ANSI X9.9, FIPS 186.3

HMAC — TLS/SSL, IPSec, SSH

HMAC-SHA256
HMAC-SHA512
HMAC-...
HMAC-SHA3 *

$$HMAC: S(k,m) = H(k \oplus opad \,||\, H(k \oplus ipad \,||\, m))$$

~~$H(k||m)$~~

Zastosowania cywilne

PRNG

- rand glibc

$r[i] = r[i-1] + r[i-30] \% p$

f. haszująca

$h(x) = x \% p$

Bezpieczeństwo / kryptografia

PRNG

szyfr strumieniowy

~~rand~~ – nieprzewidywalność, przewidywanie po kilkuset bitach

$h(x) = x \% p$ – brak kolizji

$x \neq x'$ $h(x) = h(x')$ $x' = x + p$

Kryptograficzne funkcje haszujące

~~SHA-1~~
SHA-256
SHA-512
SHA3

$h: \{0,1\}^* \longrightarrow \{0,1\}^n$

$h: D \to V$

$n > 160$ Keccak

- collision resistance

$x \neq y \quad h(x) = h(y)$

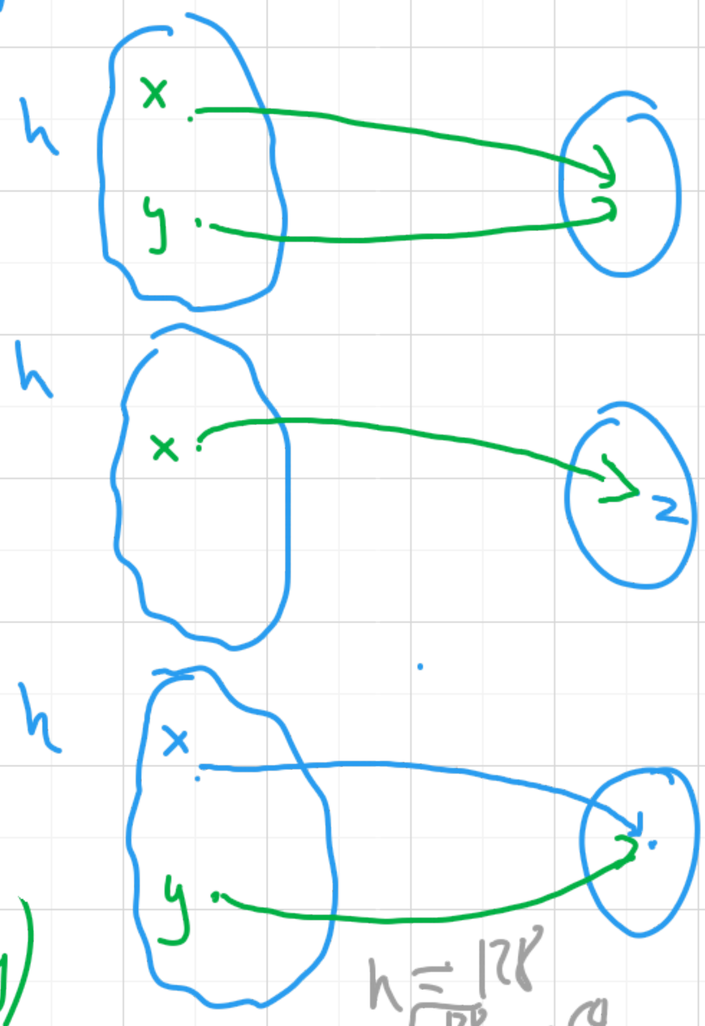
$h \longrightarrow x, y : x \neq y \wedge h(x) = h(y)$

- preimage resistance

$h, z \longrightarrow x : h(x) = z$

- 2nd preimage resistance

$h, x \longrightarrow y : y \neq x \wedge h(x) = h(y)$



$h = 128$

$m = \sqrt{2^{128}} = 2^{64}$

Birthday Paradox

Generic Birthday Attack

$h(x)$ = dzień urodzin

D - ludzie

V - dni roku $|V| = 365$

$x_1, x_2 \ldots x_{23}$

$P[\exists i \neq j : h(x_i) = h(x_j)] \geq \frac{1}{2}$

$x_1 \ldots x_{30}$

$\left(1 - 1 \cdot \frac{364}{365} \cdot \frac{363}{365} \ldots \frac{335}{365}\right) \sim 70\%$

$x_1, \ldots, x_m$

$P[\exists i \neq j : h(x_i) = h(x_j)] \sim \frac{1}{2}$ $m \sim \sqrt{|V|}$

$m \sim \sqrt{2^n} = 2^{\frac{n}{2}}$

Availability

upload m

A, X, G, timestamp

tmpName

view m'

komisji 25 000
probek 3
75 000

rand(10000, 10 000 000)

$m \sim \sqrt{10\,000\,000} \sim 3000$