One Time Pad (OTP)

szyfr Vernama 1919

wiadomość m_1 1101010111 m_2 0110110011

klucz k 1011001001 k 1011001001

kryptogram c_1 0110011110 c_2 1101111101

$c_1 = m_1 \oplus k$

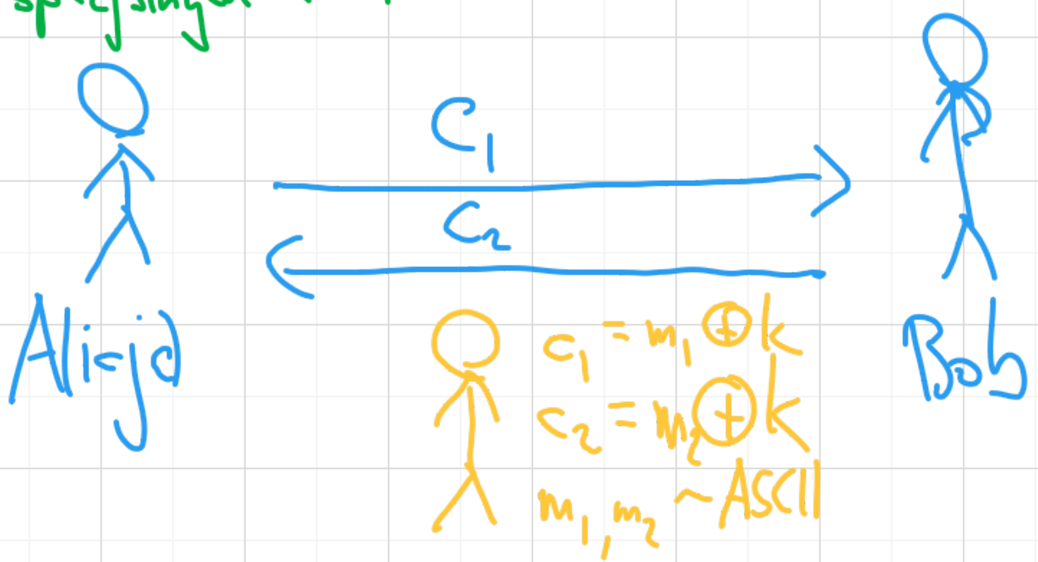
$c_2 = m_2 \oplus k$

$c_1 \oplus c_2 = (m_1 \oplus k) \oplus (m_2 \oplus k) = m_1 \oplus m_2$

ASCII $L = 100$

"litery" ≥ 64 spacja $= 32$

wiele znaków specjalnych < 64



$c_1 \oplus c_2 = m_1 \oplus m_2$

$m_1 = 0\,1\,1\,0\,0\,1\,0\,0$

$k = 1\,0\,1\,1\,0\,0\,1\,0$

$c_1 \quad 1\,1\,0\,1\,0\,1\,1\,0$

$m_2 = 0\,0\,1\,0\,0\,0\,0\,0$

$k = 1\,0\,1\,1\,0\,0\,1\,0$

$c_2 \quad 1\,0\,0\,1\,0\,0\,1\,0$

$c_1 \oplus c_2$ / $m_1 \oplus m_2$ $\quad 0\,1\,0\,0\,0\,1\,0\,0$

Lista 3

m_1 = ELA MIALA KOTA

m_2 = DZISIAJ ODNOTOWANO 19° W

m_3 = O GODZINIE 10:15 WYKLAD

k

Dane: $c_i = m_i \oplus k$

c_1 = ...

c_2 =

c_3

c_4

OSINT

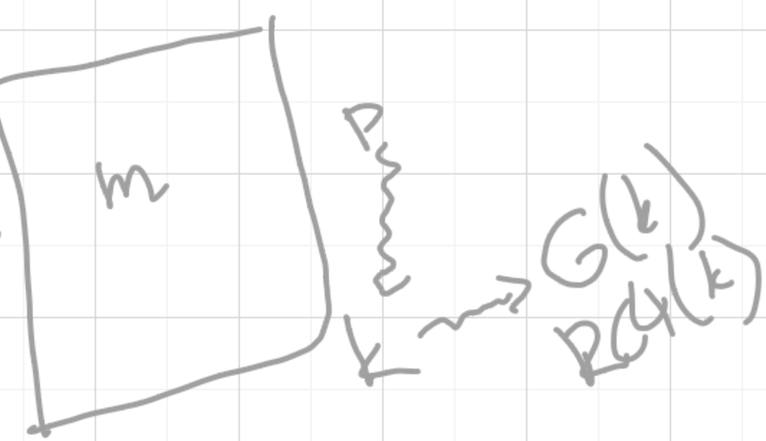
MS Excdc

MS W.xd

$c_1 = RC4(k) \oplus m_1$

$c_2 = RC4(k) \oplus m_2$

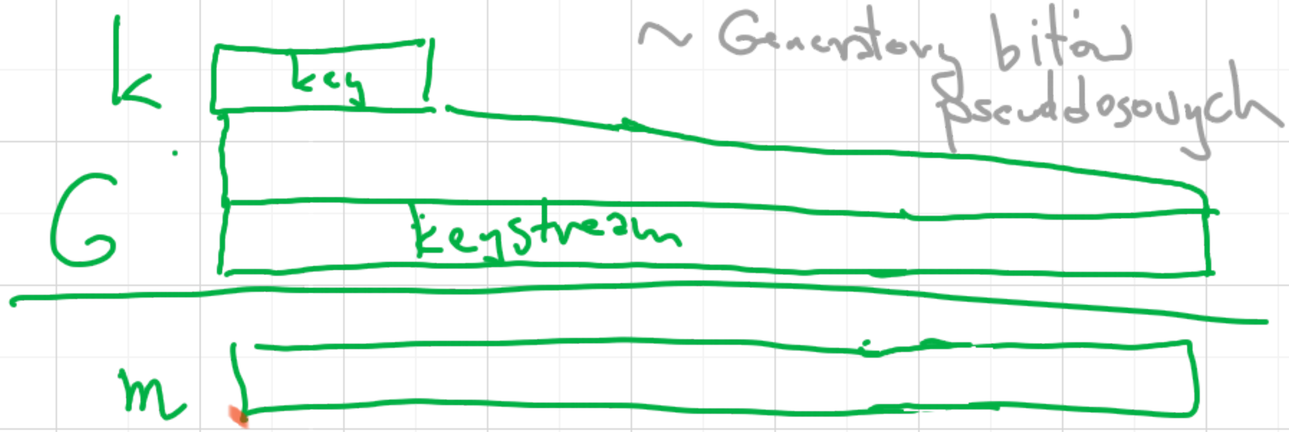
$c_3 = RC4(k) \oplus m_3$



ONE TIME PAD
(TAJNOŚĆ DOSKONAŁA)

SZYFRY STRUMIENIOWE

~ Generatory bitów pseudolosowych



jakie własności

PROBLEMY: $c = m \oplus k$

① klucz jest jednorazowy ✓ $(IV, G(IV,k) \oplus m)$

② klucz musi być tak długi jak wiadomość

$G(k) \oplus m$

$c = m \oplus G(k)$ powinno mieć G?

G-PRNG

Pseudo random Number Generator

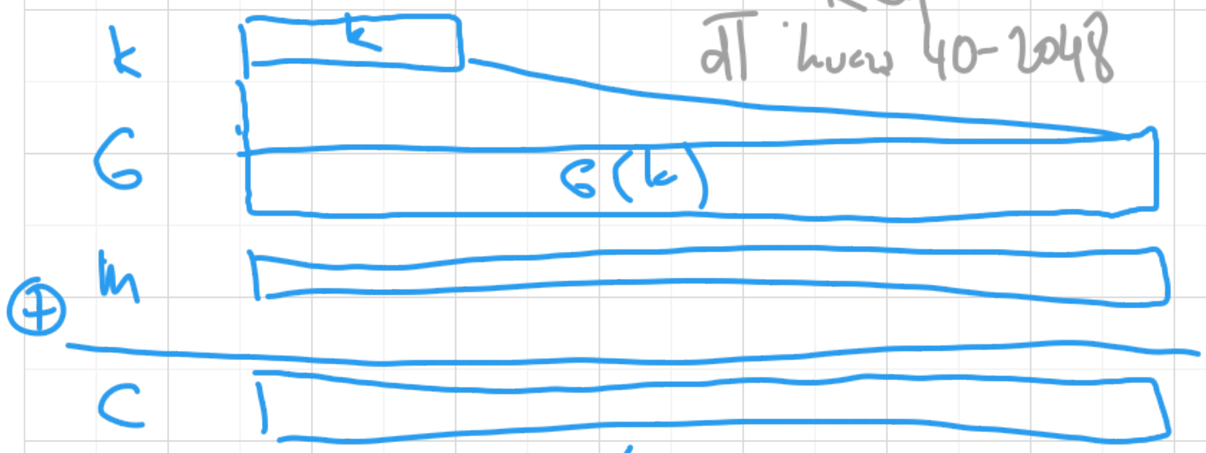
$P[A(G(k)_{1..n}) = G(U_{n+l})] \leq \frac{1}{2} + \epsilon(n)$ - pomijalność $\epsilon(n) < \frac{1}{2^{80}}$

1001000100 || 0

SZYFR STRUMIENIOWY

RC4 86

dT ilucz 40-2048



$c = G(k) \oplus m$

G jest niepseudolosowa

$k \in \{0,1\}^{128}$

$G : \{0,1\}^{l} \longrightarrow \{0,1\}^{m}$

$m > l$

2^{64} 11 128/256

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

$$\frac{(IV_1, G(IV_1, k) \oplus m_1)}{(IV_2, G(IV_2, k) \oplus m_2)} \longrightarrow$$

Współczesne szyfry strumieniowe

AES-GCM

AES-OFB

AES-...

Salsa2 (software)

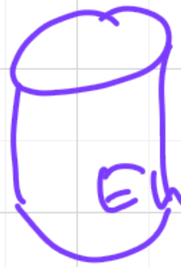
Sosemanuk (hw)

~~RC4~~

Szyfry blokowe

AES

Hello it is TDI-215



Enter username

username: wolf password: asd123

m_1

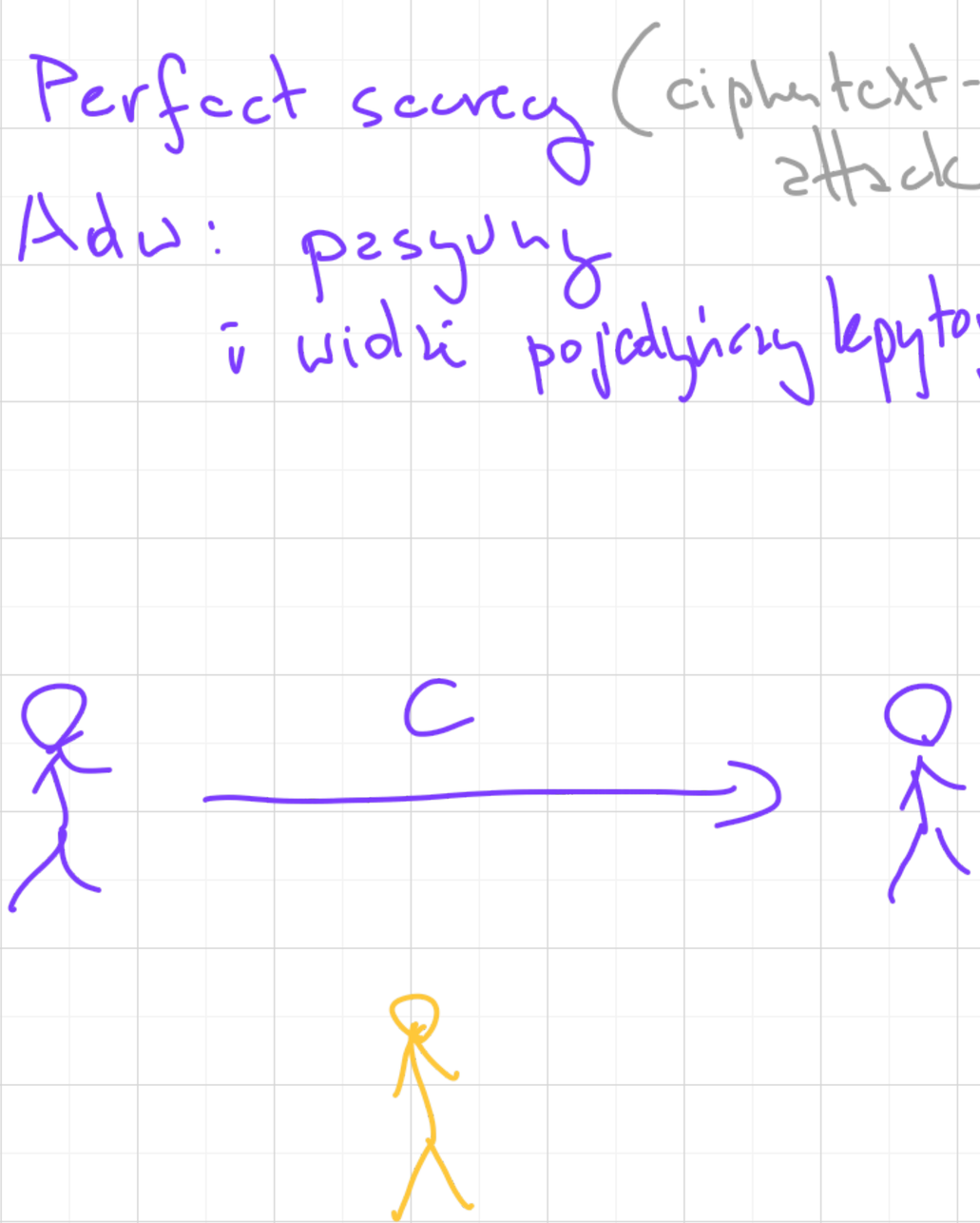
$C_1 = m_1 \oplus G(k)$

m_2

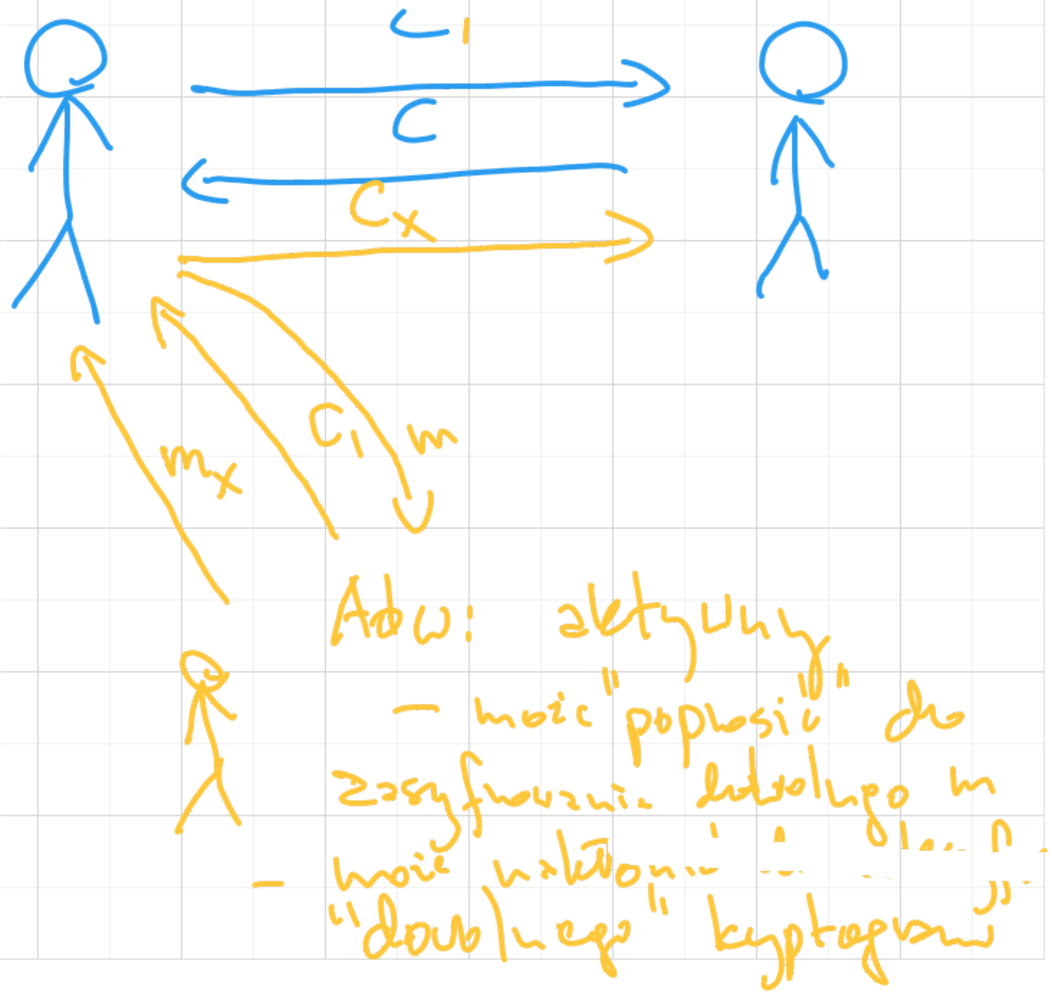
$C_2 = m_2 \oplus G(k)$

Perfect secrecy (ciphertext-only attack)

Adw: pasywny
i widzi pojedynczy kryptogram



Chosen Ciphertext Attack
CCA-security



Adw: aktywny
- może "poprosić" do zaszyfrowania dowolnego m
- może wskazać "dowolnego" kryptogramu

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

Bank

Bank$_2$

From: Alice

To: Bob / EVE

Amount: 1234