

# One Time Pad (OTP)

szyfr Vernam  
1919

wiadomość	$m_1$	1101010111	$m_2$	0110110011
klucz	$k$	1011001001	$k$	1011001001
cryptogram	$c_1$	0110011110	$c_2$	1101111010

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

---

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



# ASCII

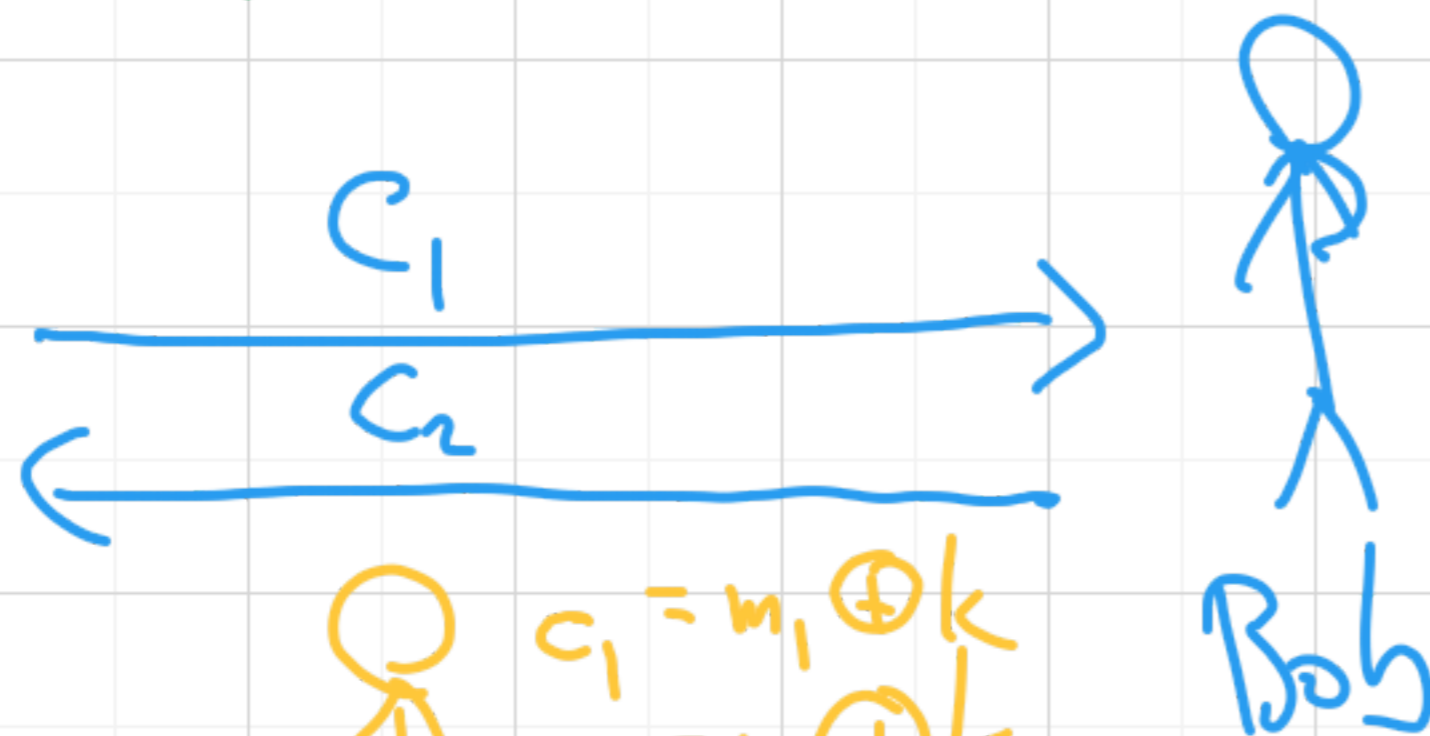
$L = 100$

"litarki"  $\geq 64$

spacje = 32

wide znaki specjalnych  $< 64$

Alija



$c_1 = m_1 \oplus k$   
 $c_2 = m_2 \oplus k$   
 $m_1, m_2 \sim \text{ASCII}$

$$c_1 \oplus c_2 = m_1 \oplus m_2$$

$m_1 = 01100100$

$k = 10110010$

$c_1 = 11010110$

$m_2 = 00100000$

$k = 10110010$

$c_2 = 10010010$

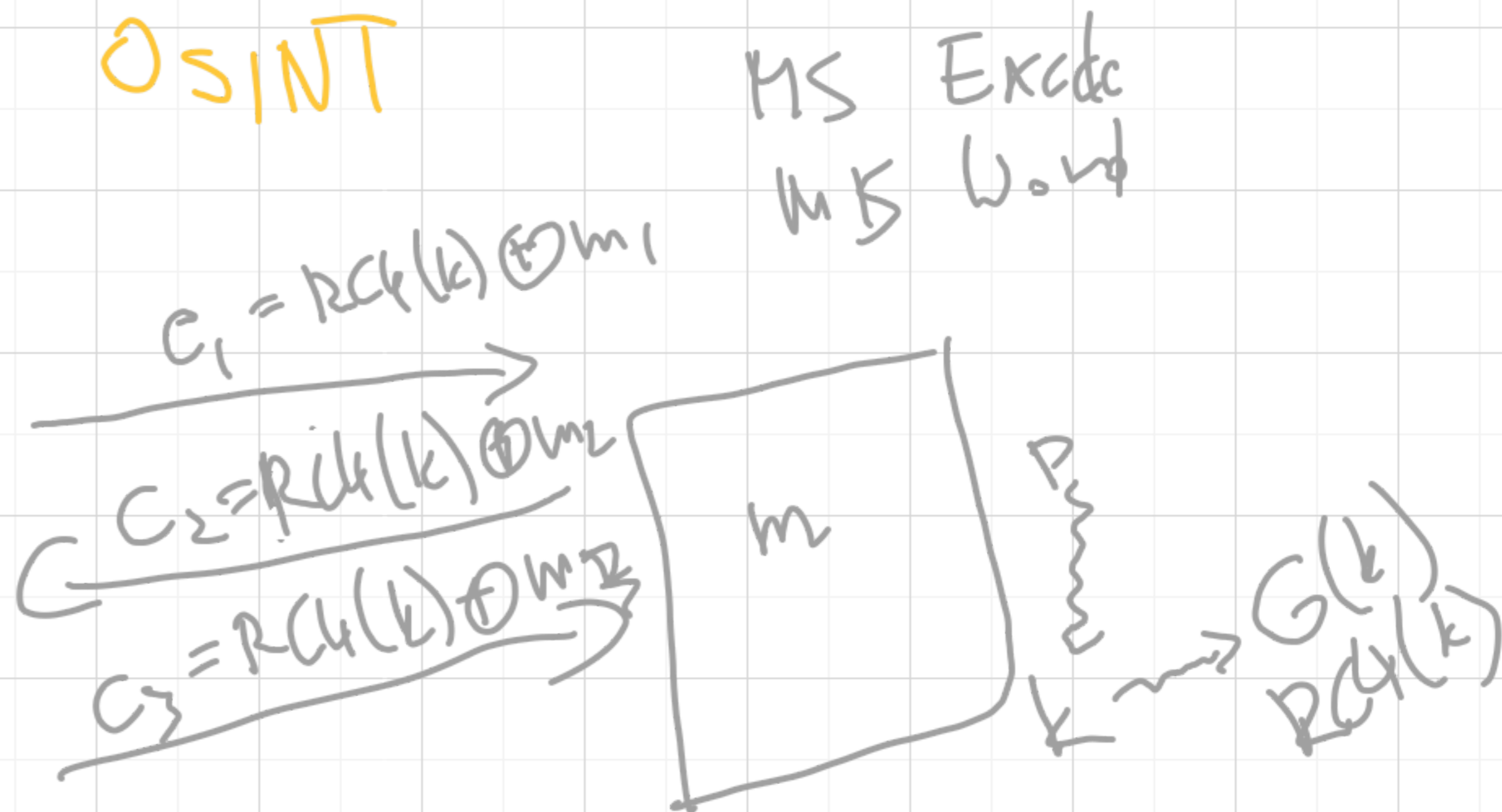
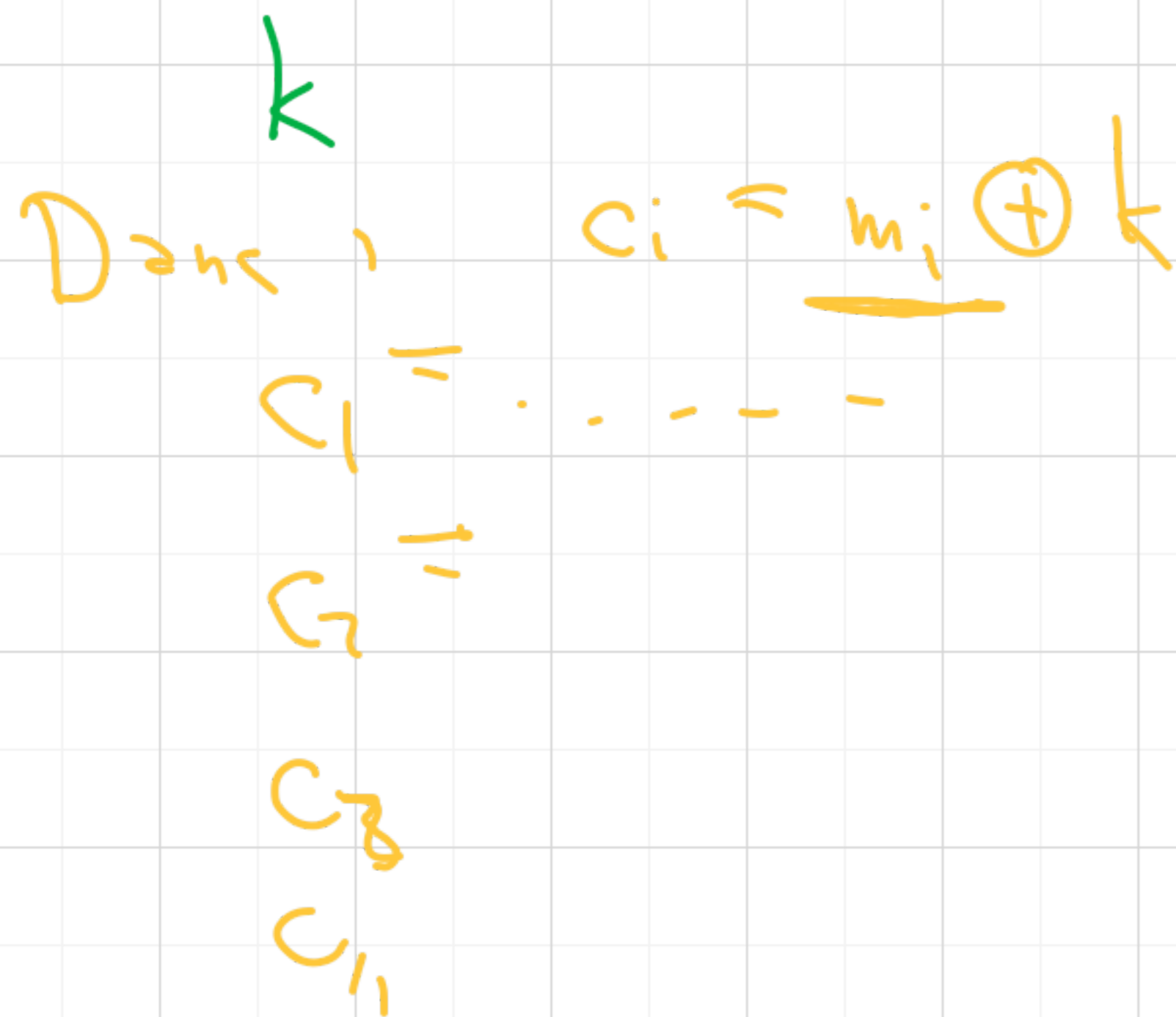
$c_1 \oplus c_2$   
 $m_1 \oplus m_2$   
 $01000100$

# Lista 3

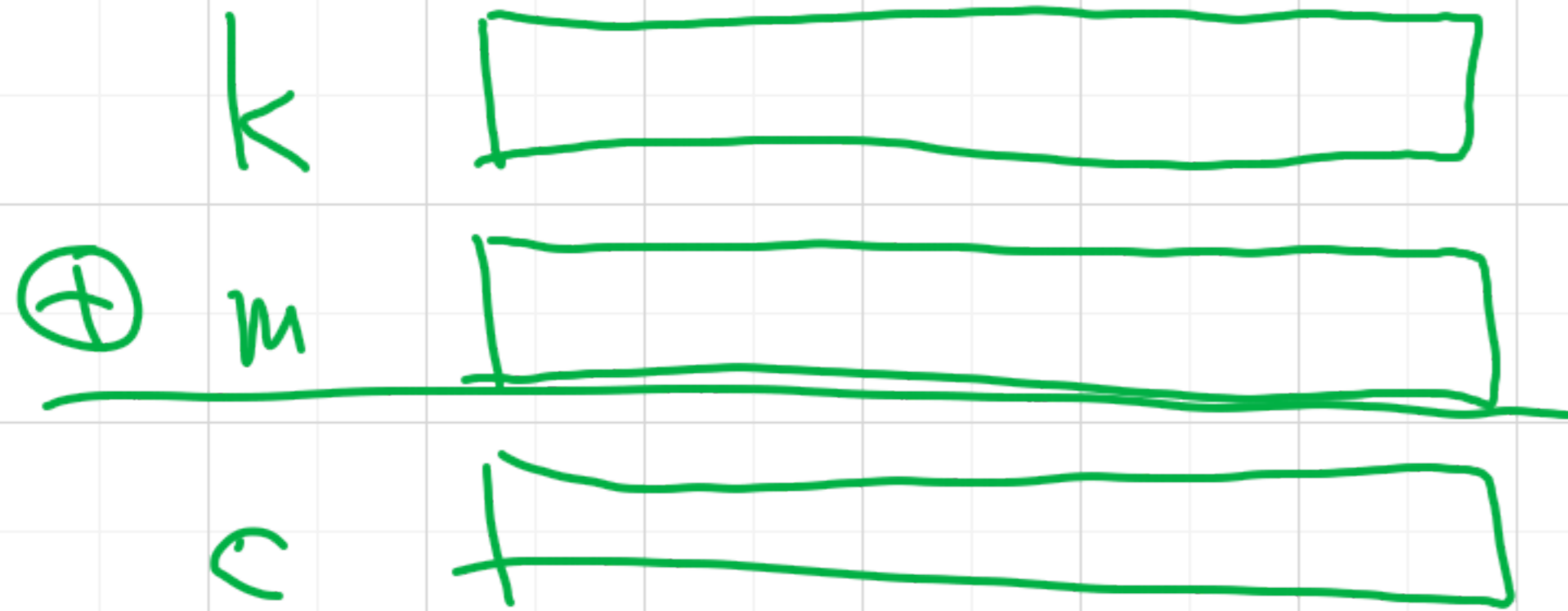
$m_1 = \text{ELA MIALA KOTA}$

$m_2 = \text{DZISIAJ ODNOTOWANO } 19^\circ \text{ W}$

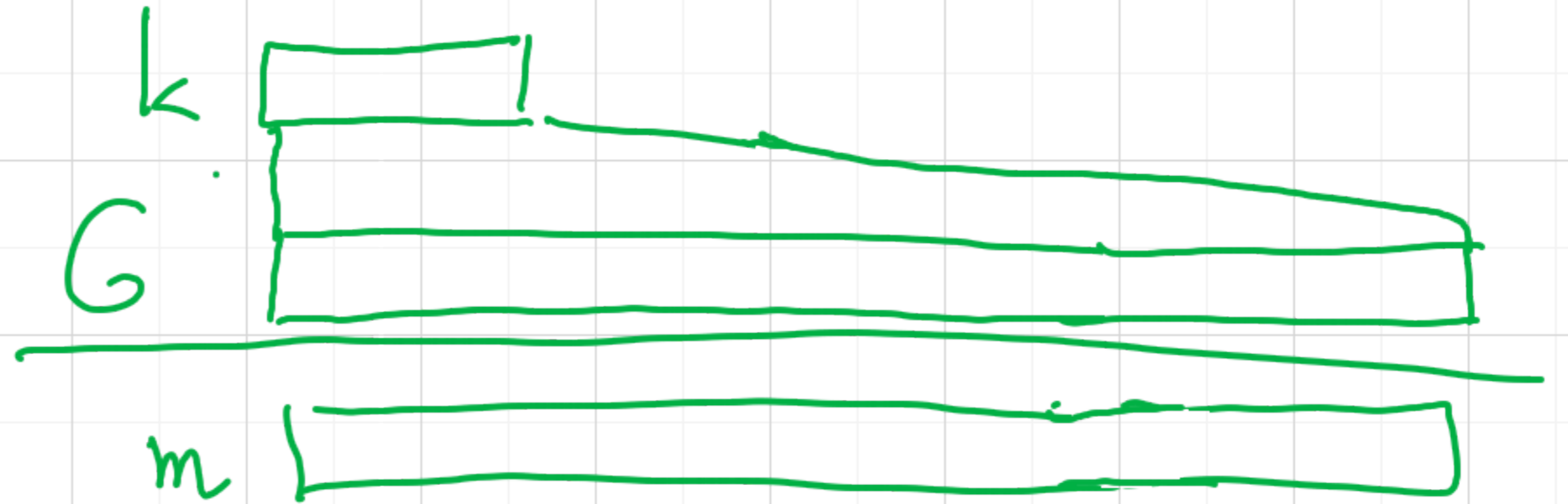
$m_3 = \text{O GODZINIE } 10:15 \text{ WYKLAD}$



# ONE TIME PAD (TAJNOŚĆ DOSKONAŁA)



# SZYFRY STRUMIENIOWE



PROBLEMY:  $c = m \oplus k$

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

② klucz musi być tak długi jak wiadomość ✓  
 $G(k) \oplus m$

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

jakie własności powinno mieć  $G$ ?

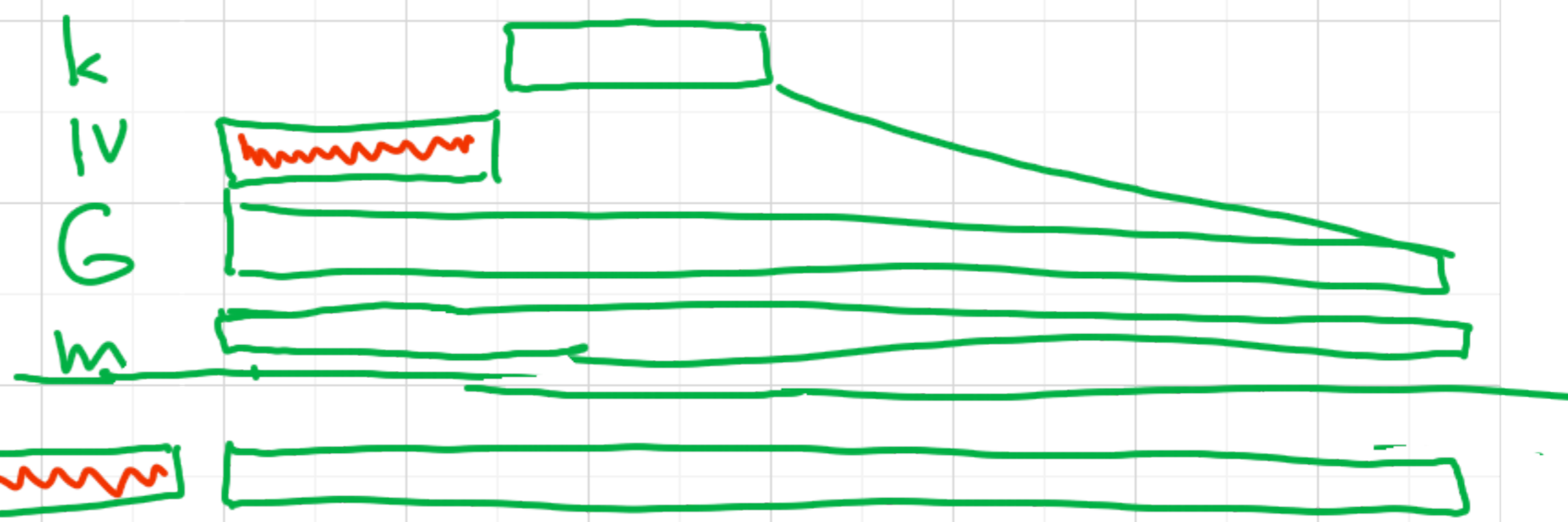
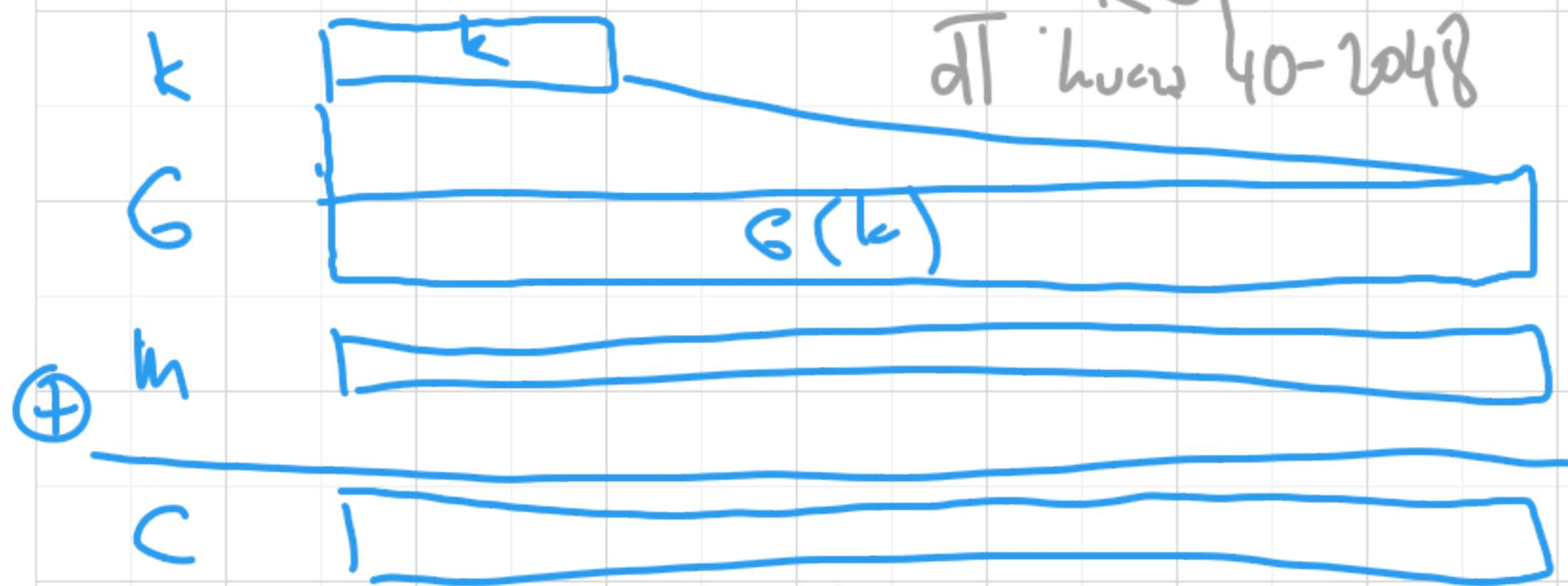
G-PRNG  
Pseudo random

$$P[A(G(k), \dots, n) = 1] \leq \frac{1}{2^{\text{te Number Generator}}}$$

1001000100 // 01  
 $\epsilon(n) - \text{poziomy} \text{ } \epsilon(n) < \frac{1}{2^{80}}$

# SZYFR STRUMIENIOWY

RC4 86  
 dT liczą 40-2048



$c = G(k) \oplus m$   
 G jest nieprzewidywalna  
 $k \in \{0, 1\}^{128}$   
 $G: \{0, 1\}^l \rightarrow \{0, 1\}^m$   
 $m > l$   
 $2^{64}$        $128/256$

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

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



Współczesne szyfry strumieniowe

AES-GCM

AES-OFB

AES-...

Salsa2 (software)

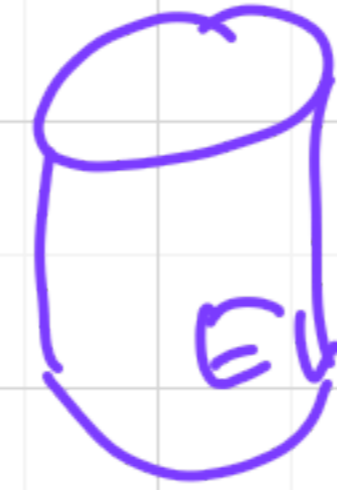
Sosemanuk (hw)

Szyfry blokowe

AES



← Hello it is TDI-215



Enter username

username: wolf password: zsd123 →

$m_1$   
 $C_1 = m_1 \oplus G(k)$

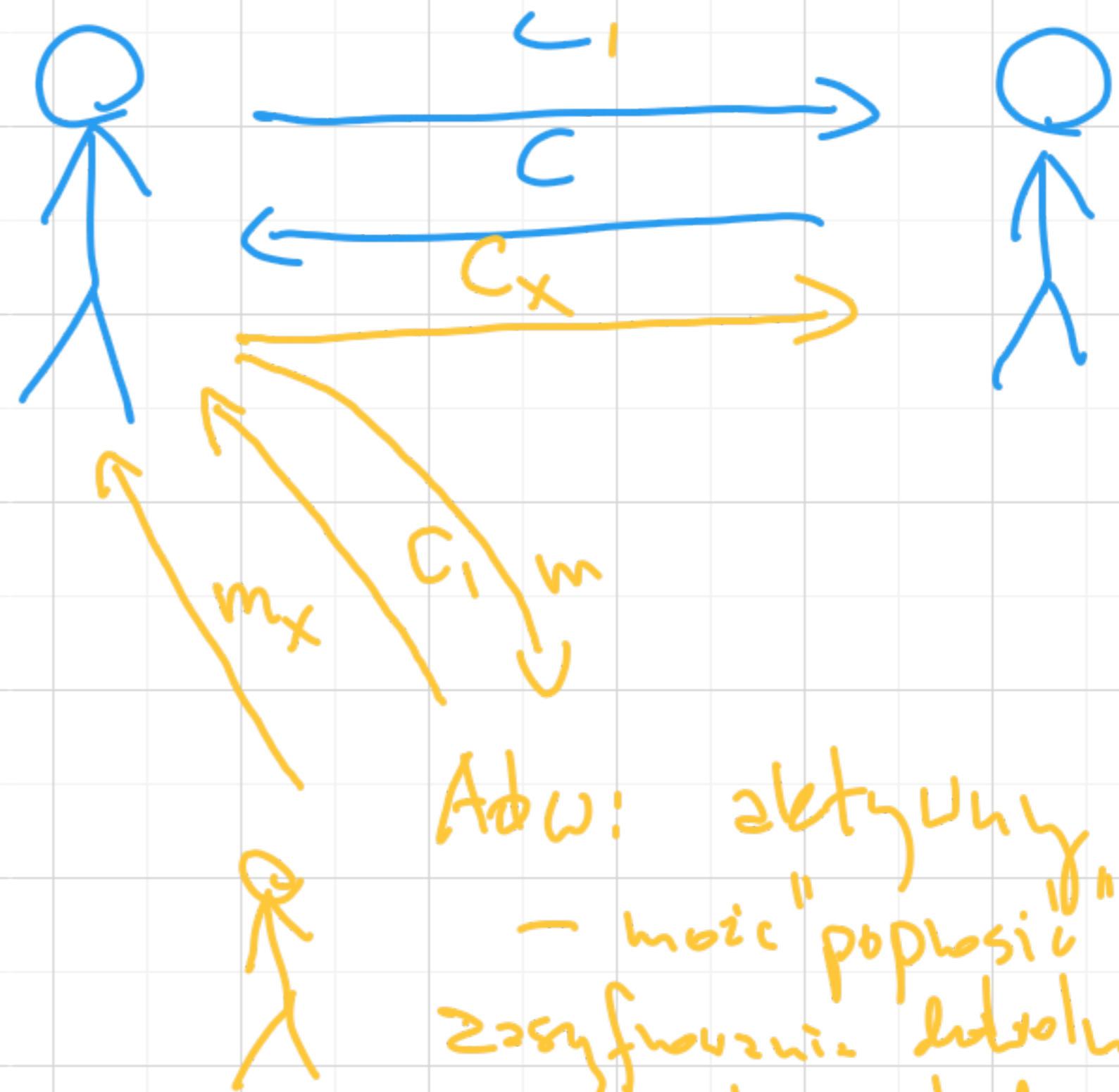
$m_2$   
 $C_2 = m_2 \oplus G(k)$

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 nakłonić do "dobrego" kryptogramu



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

Bank 1

Bank 2

From: Alice

To:

Amount:

Bob  
Eve

1 2 3 4

1000100100010

[ ]

