

symmetric block

plaintext

key



64 bits (128)



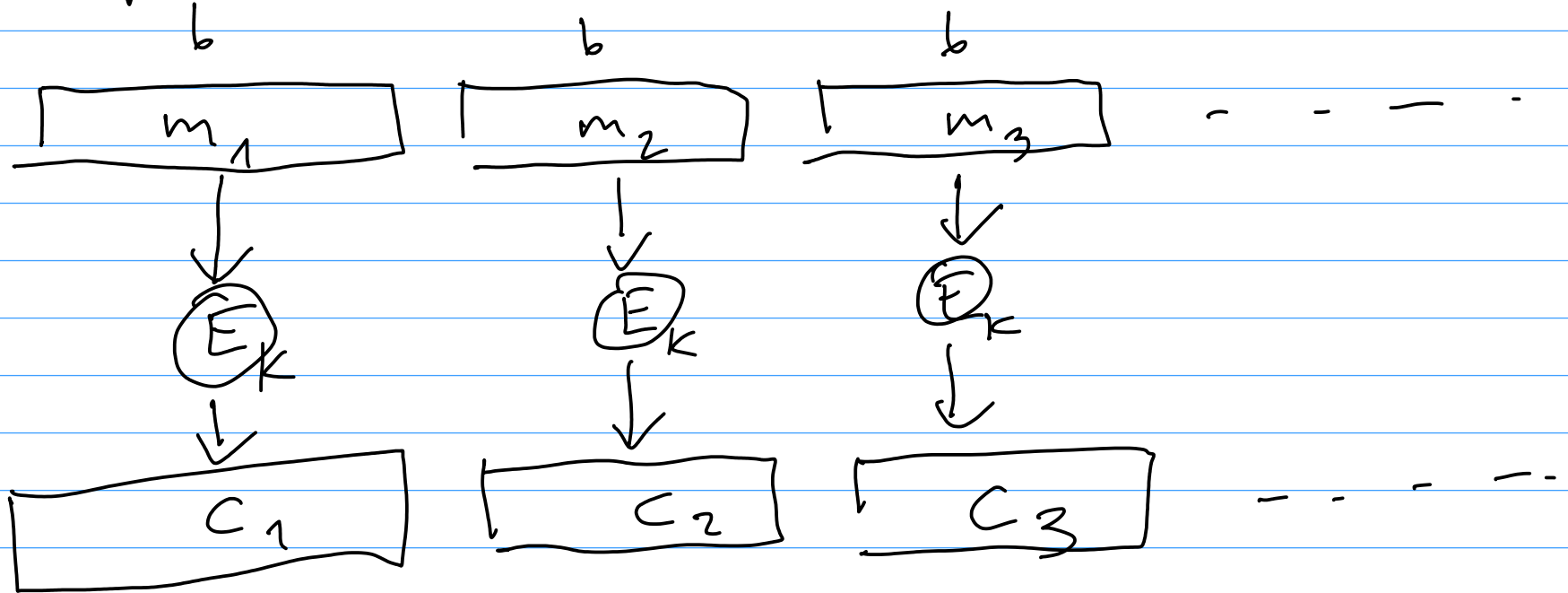
$E_K$



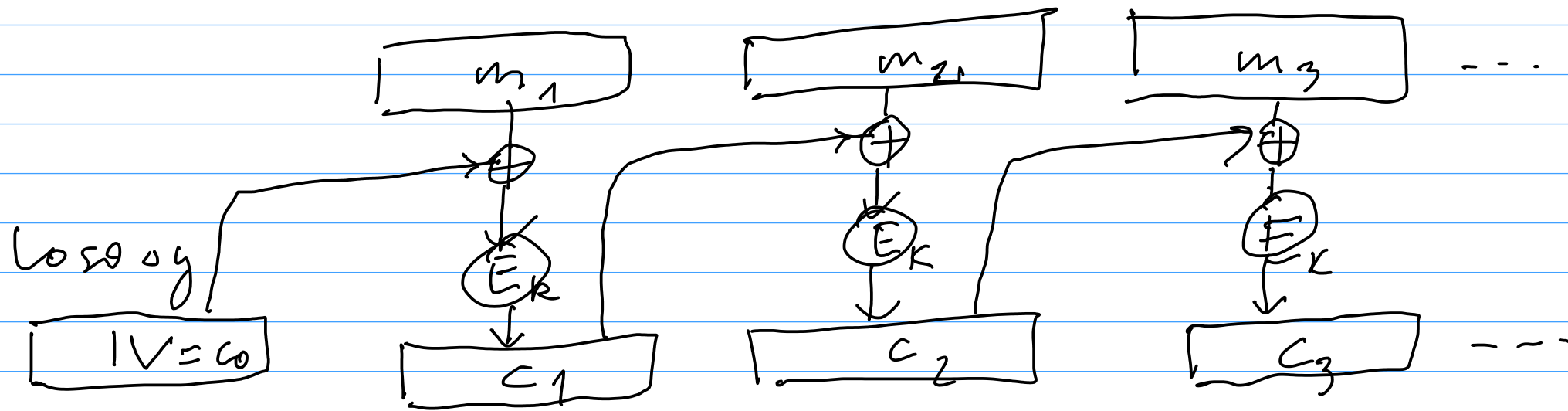
64 bits

ciphertext

Typ ECB (Electronic Codebook)



# Tryb CBC (Cypher Block Chaining)

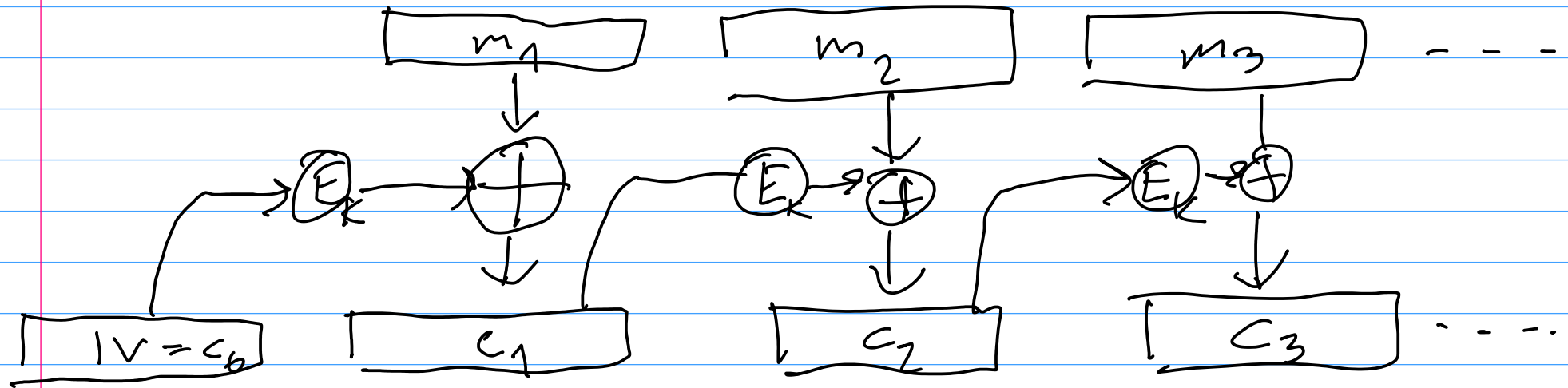


Initial vector

$$C_i = E_K(m_i \oplus C_{i-1})$$

$$m_i = D_K(C_i) \oplus C_{i-1}$$

Tryp CFB (Cipher Feedback)



$$c_i = E_k(c_{i-1}) \oplus m_i$$

$$m_i = E_k(c_{i-1}) \oplus c_i$$

# Typ OFB (Output Feedback)

Szyfrowanie strumieniowe

One time pad  $\oplus$   $\begin{array}{ccccccc} m_1 & m_2 & m_3 & - & - & - \\ r_1 & r_2 & r_3 & - & - & - \\ \hline c_1 & c_2 & c_3 & - & - & - \end{array}$

W szyfrowaniu strumieniowym

$r_1 r_2 r_3 - \dots$  nie jest kluczem

tylko jest produkowane przez

generátor pseudo losowy przy użyciu  
tajnego klucza  $K$

$$K \downarrow$$

$$\boxed{gen} \rightarrow r_1 r_2 r_3 - - - -$$

A

$$\oplus \begin{array}{ccccccc} & m_1 & m_2 & m_3 & - & - & - \\ & r_1 & r_2 & r_3 & - & - & - \\ \hline & c_1 & c_2 & c_3 & - & - & - \end{array}$$

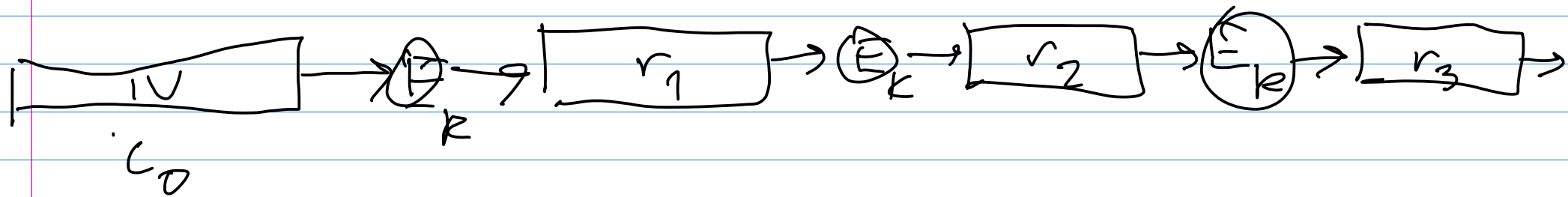
B

$$K \downarrow$$

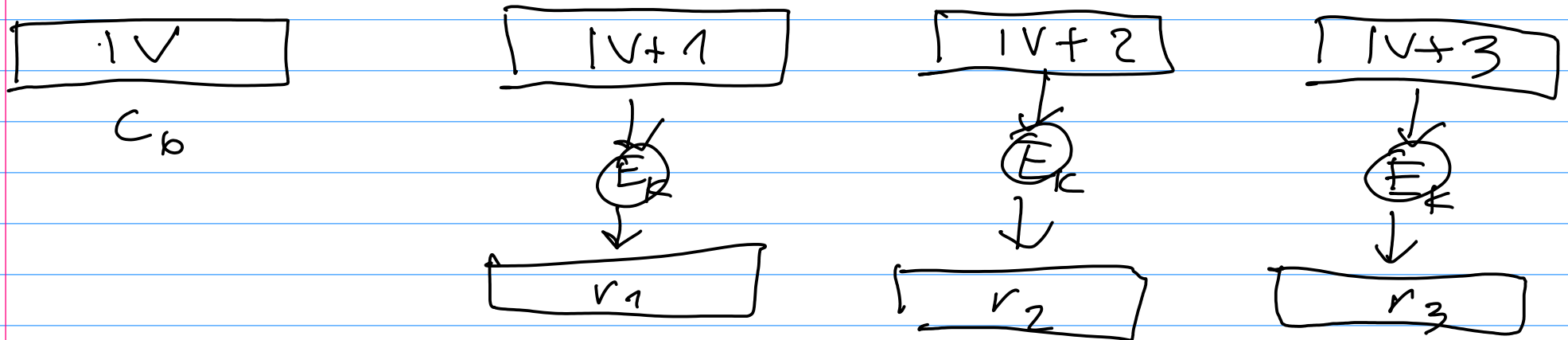
$$\boxed{gen} \rightarrow r_1 r_2 r_3 - - - -$$

$$\oplus \begin{array}{ccccccc} & c_1 & c_2 & c_3 & - & - & - \\ & r_1 & r_2 & r_3 & - & - & - \\ \hline & m_1 & m_2 & m_3 & - & - & - \end{array}$$

OFB

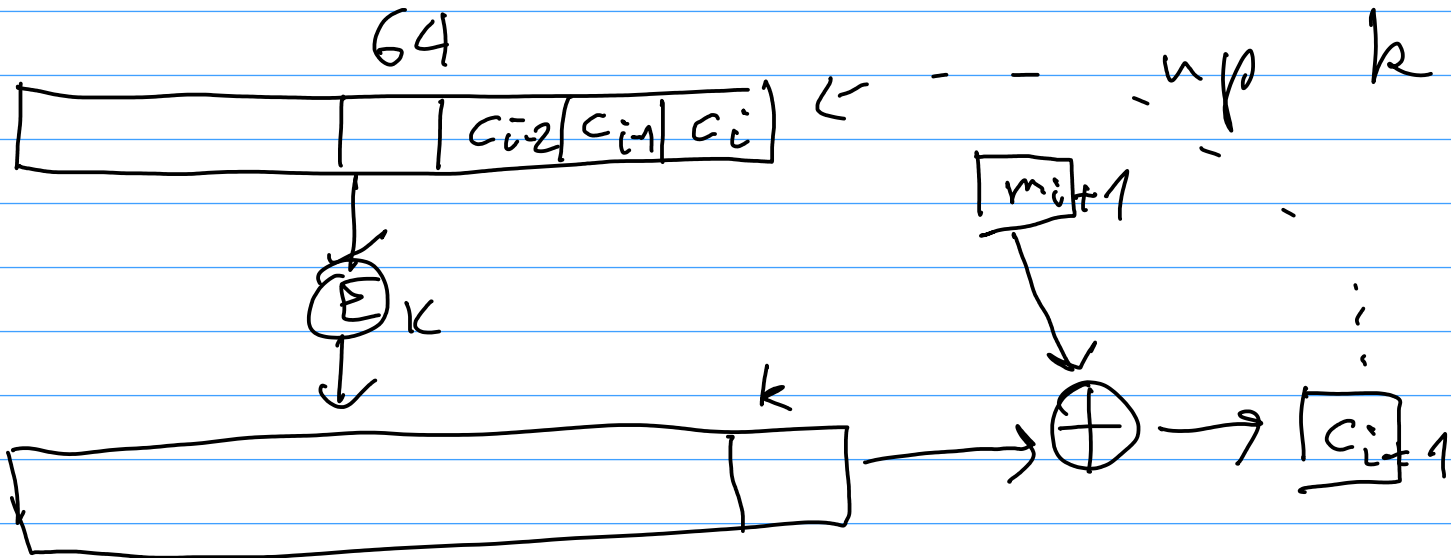


CTR (Counter mode)

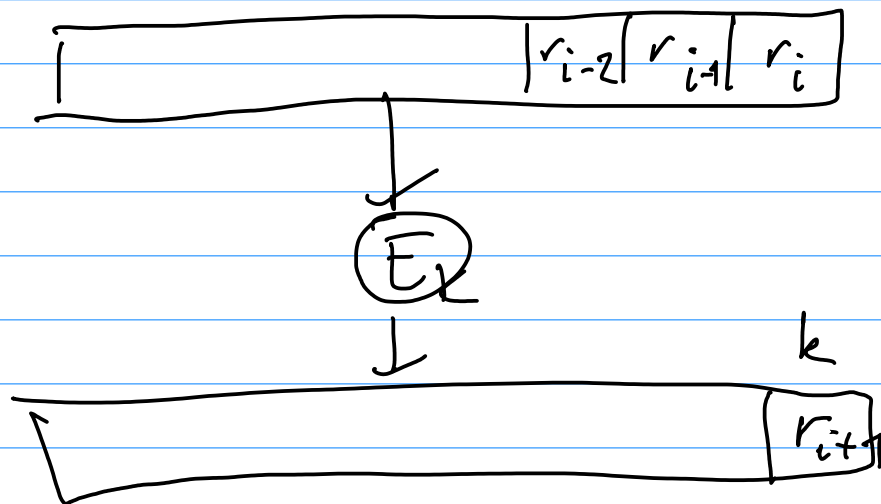


k-CFB

mesytanie bloki, k-bit



k-OFB





Kryptanaliza DES

Obecnie najprostszym sposobem  
jest przeszukiwanie przestrzeni  
wszystkich kluczy.

Kryptanaliza różnicowa

Kryptanaliza liniowa

3-DES

$$C = E_{K_1} D_{K_2} E_{K_3}(m)$$

Dla czego wie 2-DES?  $C = E_{K_1} E_{K_2}(m)$

Attack Meet in the Middle

$m_1 m_2 m_3$

$c_1 c_2 c_3$

$E_{K_2}(m_1) E_{K_2}(m_2) E_{K_2}(m_3)$

$D_{K_1}(c_1) D_{K_1}(c_2) D_{K_1}(c_3)$

$\forall K_2$  obł. porównaj trójki  
wyniki sortujemy

$\forall K_1$  obł. tak trójki  
wyniki sortujemy

odp  $(k_1, k_2)$

$k_2$

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

\_\_\_\_\_

$k_1$

Bezpieczeństwo alg symetryczny w  
sensie LOR (Left or right)

Dany jest pewien alg symetryczny  
 $E_K(\cdot)$

Algorytm ten jest bezpieczny w sensie  
LOR gdy nie możemy odróżnić  
2 maszyn symetrycznych:

$$O_0(m_0, m_1) = E_K(m_0)$$

$$O_1(m_0, m_1) = E_K(m_1)$$

Przykład: ECB nie jest bezpieczny  
✓ sensie LOR

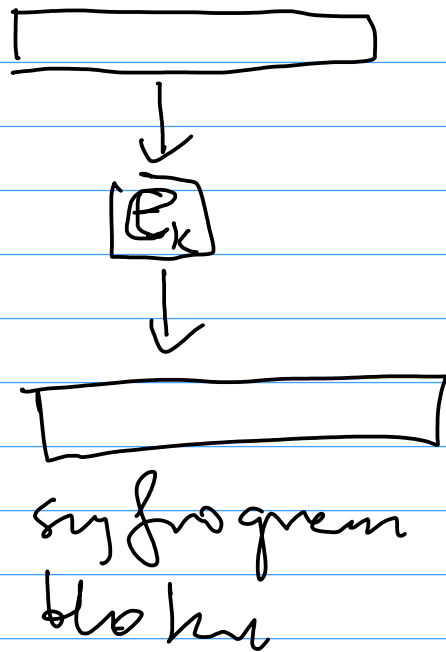
$$O_i(M_0, M_0) = E_K(M_0)$$

$$O_i(M_1, M_1) = E_K(M_1)$$

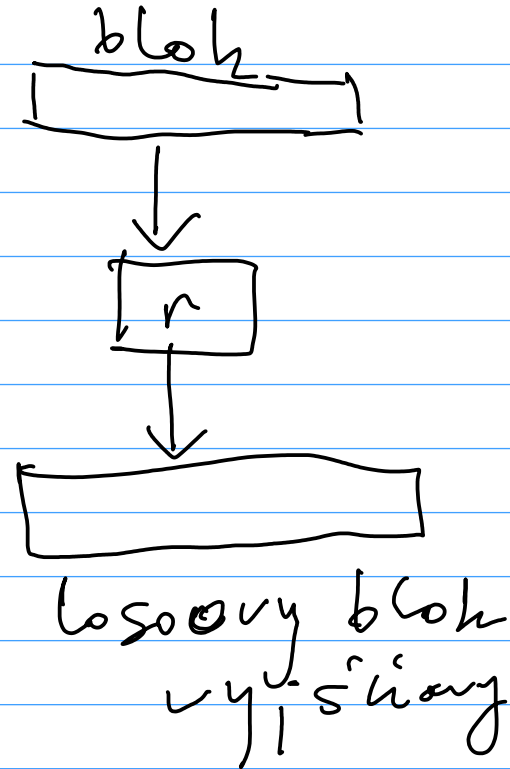
$$O_i(M_0, M_1) = E_K(M_i)$$

Tu typ CBC jest bezpieczny  
✓ sensie LOR (jest system  
blokowy na którym działa)

Szyfr blokowy



maszyna losująca



Szyfr blokowy jest bezpieczny gdy  
nie można go odnieść od maszyny  
losującej

Def

$e_k$  jest bezpieczny test dla  
dowolnego algorytmu  $A$  który  
działa  $\vee$  max czasie  $T$   
i odwołuje się do  $e_k$  (lub  $v$ )  
max  $L$  razy ( $A$  zwraca  $0$  lub  $1$ )

$$|Pr(A(e_k)=1) - Pr(A(v)=1)| < \varepsilon$$

$E_k$  jest bezpieczny w sensie ROR  
gdy nie można odróżnić 2 wyzorni

$$E_k(M) \text{ i } E_k(R(M))$$

gdzie  $R(M)$  to losowy ciąg o  
tej samej długości co  $M$

ROR to skrót od Random or Real

Tu  $E_k$  jest bezpieczny w sensie

LOR  $\Leftrightarrow E_k$  jest bezpieczny w

sensie ROR



LOR

$\forall$  A diaľajčery v strane T i  
vykonajčery syfrovane l bloh  
(A zvraca 0 v 1)

$$|Pr(A(O_0)=1) - Pr(A(O_1)=1)| < \varepsilon$$

ROR

$$|Pr(A(E_K)=1) - Pr(A(E_K(R))=1)| < \varepsilon$$

$$O_0(m_0, m_1) = E_{1c}(m_0)$$

$$O_1(m_0, m_1) = E_K(m_1)$$

$$O_2(m_0, m_1) = E_K(R(m_0))$$

$Z_{\text{OT}}$  i  $\text{syfr}$  jest bezpieczny  $\vee$  sensywny  
 $R_{\text{OK}}$  i  $\text{pochozmy}$   $\text{ze}$  jest bezpieczny  
 $\vee$  sensywny  $L_{\text{OK}}$

$$\begin{aligned}
 & \left| \Pr(A(\mathcal{O}_1) = 1) - \Pr(A(\mathcal{O}_0) = 1) \right| = \\
 & \left| \Pr(A(\mathcal{O}_1) = 1) - \Pr(A(\mathcal{O}_2) = 1) + \right. \\
 & \quad \left. \Pr(A(\mathcal{O}_2) = 1) - \Pr(A(\mathcal{O}_0) = 1) \right| \leq \\
 & \left| \Pr(A(\mathcal{O}_1) = 1) - \Pr(A(\mathcal{O}_2) = 1) \right| + \\
 & \left| \Pr(A(\mathcal{O}_0) = 1) - \Pr(A(\mathcal{O}_2) = 1) \right| \leq \\
 & 2 \left| \Pr(A(E_k) = 1) - \Pr(A(E_k(k)) = 1) \right| < 2\varepsilon
 \end{aligned}$$

Założymy, że syfr jest bezpieczny  $\vee$   
sense LOR i pokazujemy że jest  
bezpieczny  $\vee$  sense ROR

Gdyby syfr nie był bezpieczny  $\vee$   
sense ROR, to można byłoby  
odróżniać  $E_K(M)$  i  $E_K(R(M))$

$\exists A$

$$|Pr(A(E_K) = 1) - Pr(A(E_K(R) = 1))| \geq \epsilon$$

$$O_0(M, R(M)) = E_K(M)$$

$$O_1(M, R(M)) = E_K(R(M))$$