OTP

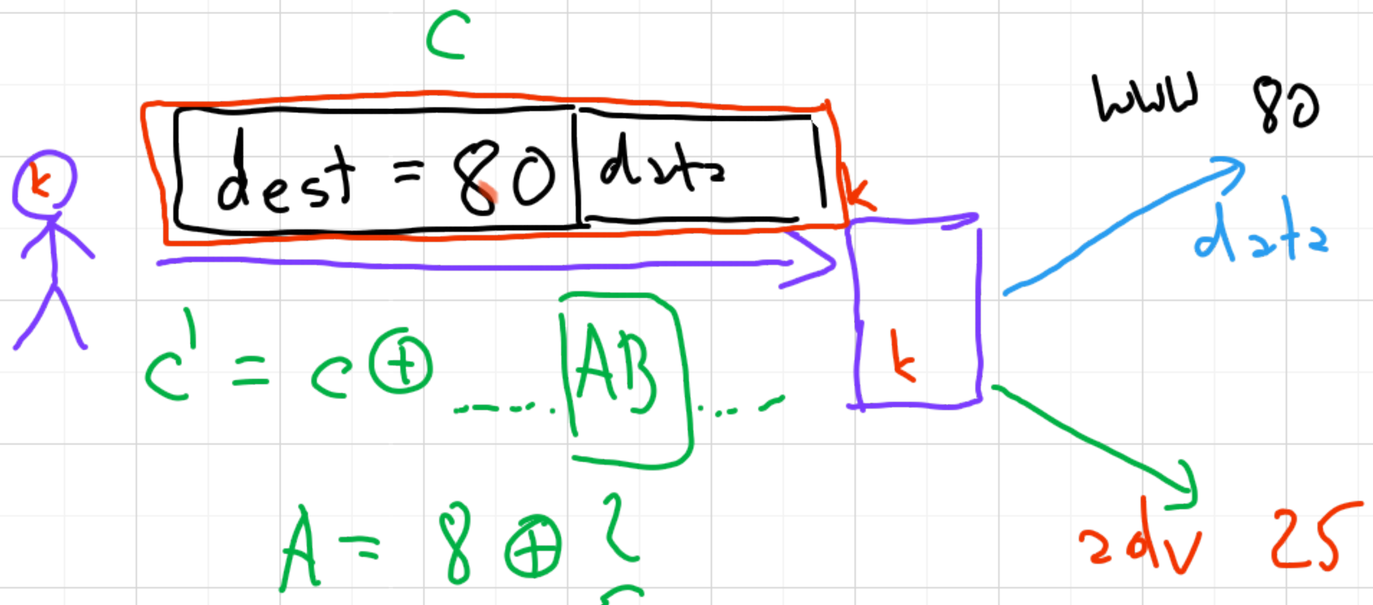
↓ krótkie klucze CPA widokowego u.

Szyfry strumieniowe

malleable

↓ odporność na CPA / CCA

Authenticated encryption



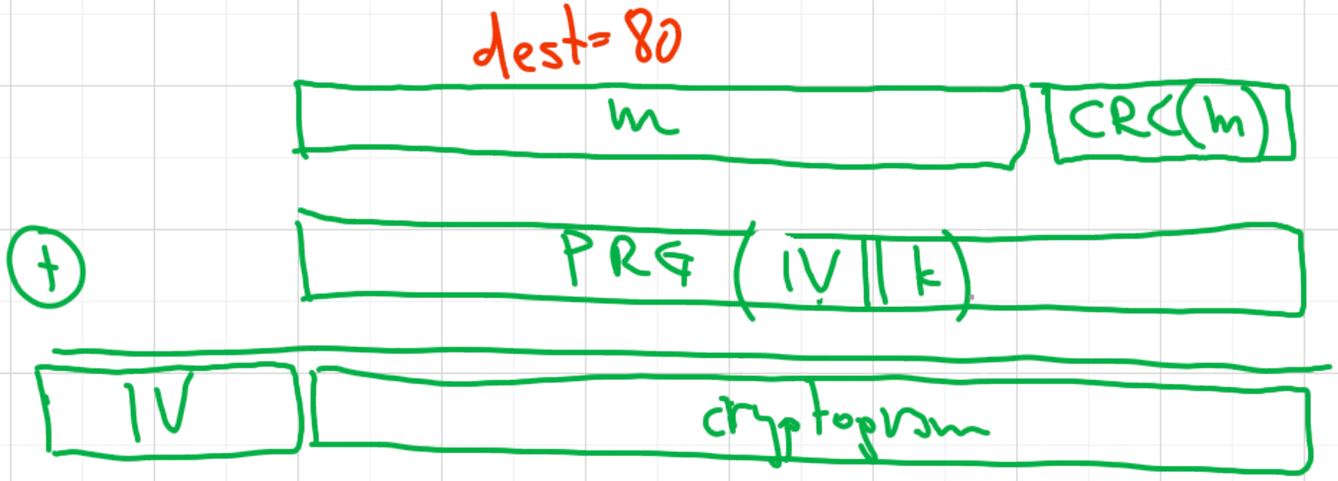
A = 8 ⊕ 2

B = 0 ⊕ 6

802.11b WEP (Wire-equivalent Privacy)

PRZYKŁAD WEP

802.11b



Atak z poprzedniego slajdu

CRC - jest liniowym m m'

$$CRC(m) \oplus CRC(m') = CRC(m \oplus m')$$

$m' =$ ..... AB ..... CRC(.. AB ....)

Inne problemy WEP

- PRG = RC4
- IV || k (128)
  - |IV| = 24 (3)
  - |k| = 104 (13)

$\Rightarrow 2^{24}$ IV się powtórzy

PRZYKŁAD

Próba konstrukcji Authenticated Encryption

MAC - $t(k, x)$ $E(k_E, m)$

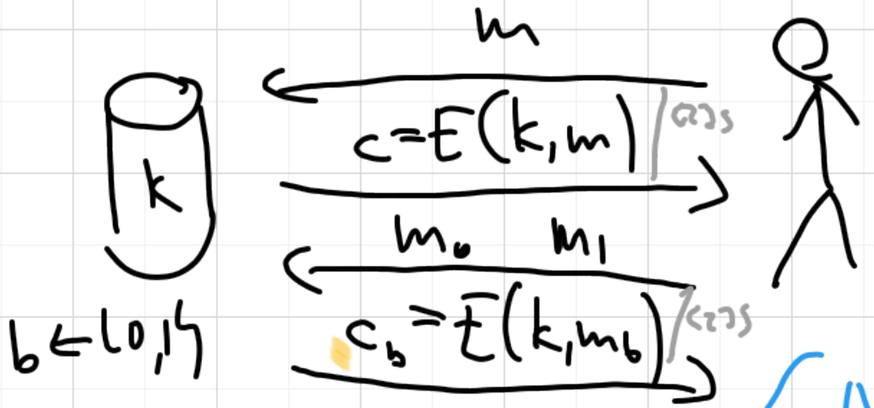
odp CCA

① SSL

② ✓ IPSEC

③ SSH

Chosen Plaintext Attack

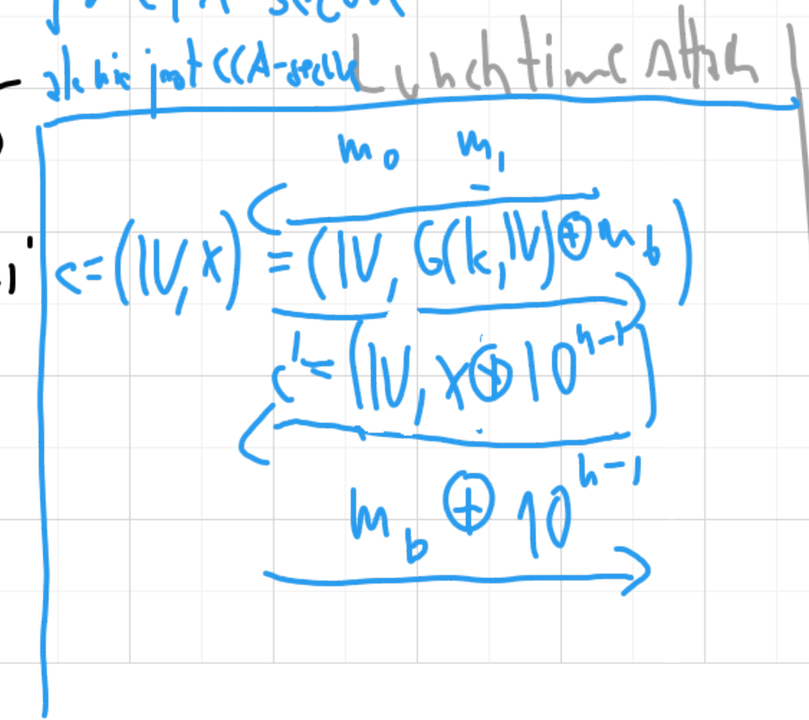


szyfr strumieniowy

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

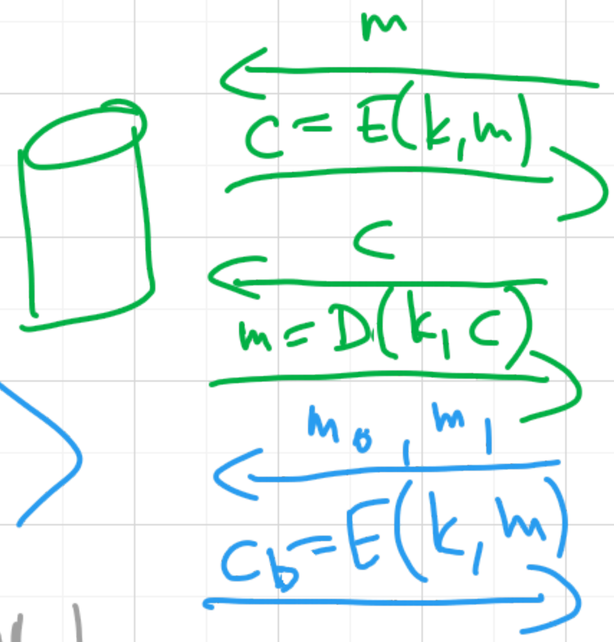
jest CPA-secure

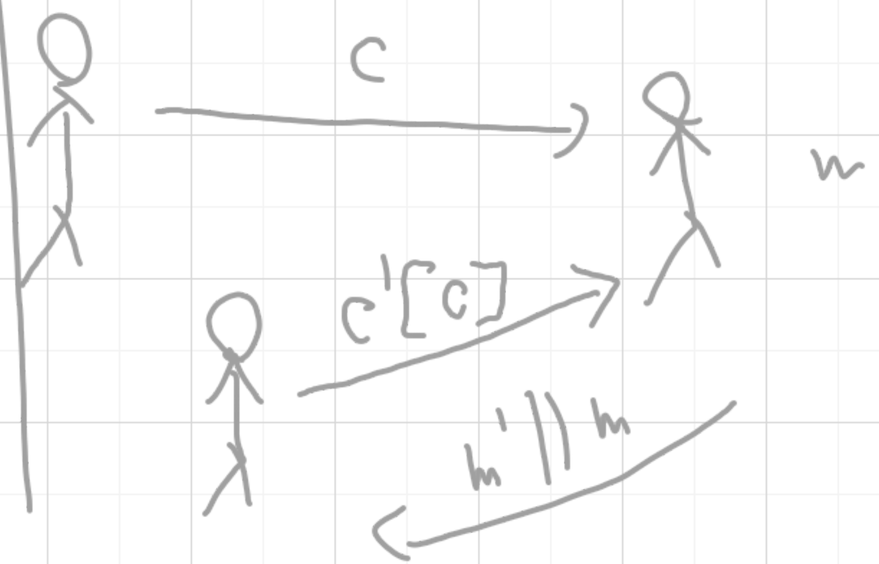
ale nie jest CCA-secure ← chosen ciphertext attack



- 1947 ..... CAS
- szyfrowanie dyskiem

Chosen Ciphertext Attack





PrzykŁad

SSH (stara wersja)
brak odporności na CCA

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

$E(k_E, m)$ $\quad$ $t = MAC(k, m)$

AE

$Enc(k, k_E, m) = (c, t)$

$c = E(k_E, m)$

$t = MAC(k, m)$

$Dec(k, k_E, (c,t))$:

$m' = D(k_E, c)$

if $Vrfy(k, m', t)$

return m'

else: $\perp$

$Enc : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$

losowe!

$Dec : \mathcal{K} \times \mathcal{C} \to \mathcal{M} \cup \{\perp\}$

gdy MAC jest deterministyczny

m_0, m_1 →

← $r_b = E(k, m_b) = (c_b, t_b)$

m_0 →

← (c, t_0)

Side-channel attacks