Private-key encryption ← k A Eve B

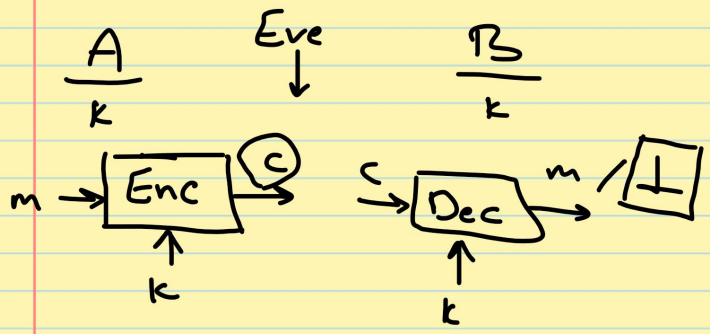
Public-key encryption →

Alice k

(Gen , Enc , Dec)

$Dec_k(c) = m$

$Enc_k(m) = c$



(Gen , Enc , Dec)

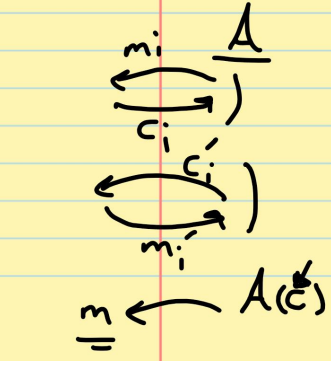
Gen: احتمالي Enc: احتمالي / حتمي Dec: حتمي

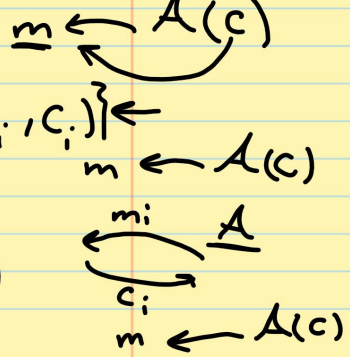
$Dec_k(Enc_k(m)) = m$

$c \longrightarrow m$

Threat model:

1. ciphertext-only attack
2. known-plaintext attack
3. chosen-plaintext attack (CPA)
4. chosen-ciphertext attack (CCA)





فرض تجزیه: $p \cdot q = N$

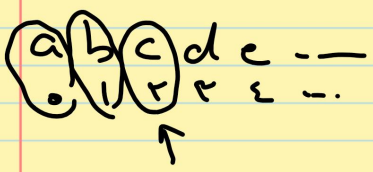
N

- رمز وبژنر:

k = cafe

m = tell him about me
cafecafecafeca

c = VE ...

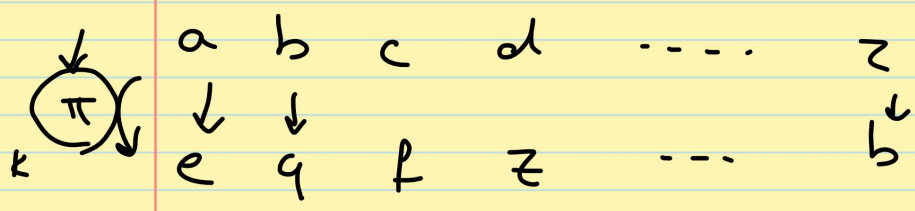


k = cafe

m : te

c a

c : VE



$m = baz \longrightarrow qebc = c$

Perfect-secrecy: (Gen, Enc, Dec) $\mathcal{M}$

$\forall m \in \mathcal{M}, \forall c \in C \quad \overline{Pr[C=c] > 0}$:

$$Pr[M=m \mid C=c] = Pr[M=m]$$

$\mathcal{M} = \{a, b, c, \ldots z\}$ (26) $Pr[M = a] = \frac{1}{26}$

$\forall m \in M, \forall c \in C \quad Pr[C=c] > 0$:

$$Pr[M=m \mid C=c] = Pr[M=m]$$

<=>

$$Pr[Enc_k(m)=c] = Pr[Enc_k(m')=c]$$

$\Pi = (Gen, Enc, Dec)$: $PrivK^{eav}_{A,\Pi}$

$m_0, m_1 \in M$ $\quad m_0, m_1 \leftarrow A$ .1

$k \leftarrow Gen$ .2

$b \xleftarrow{R} \{0,1\}$

$c \leftarrow Enc_k(m_b)$

$b' \leftarrow A(c)$ .3

$b = b'$

$$Pr[PrivK^{eav}_{A,\Pi} = 1] = \frac{1}{2}$$

perfectly indistinguishable تمایزناپذیر کامل

perfect indis. $\sim$ perfect secrecy

- One-Time Pad (OTP) → perfectly secret

$\ell > 0$, $M = K = C = \{0,1\}^{\ell}$

Gen: $k \xleftarrow{\$} K$

$Enc_k(m)$: $c = m \oplus k$

$Dec_k(c)$: $m = c \oplus k$

Thm. OTP is perfectly secret.

→ $Pr[M=m \mid C=c] = Pr[M=m]$

→ $Pr[C=c \mid M=m] = Pr[Enc_k(m)=c] = Pr[m \oplus k = c]$

$= Pr[k = m \oplus c] = \frac{1}{2^{\ell}} = 2^{-\ell}$

(*) $Pr[M=m \mid C=c] = \frac{Pr[C=c \mid M=m] \cdot Pr[M=m]}{Pr[C=c]}$

$Pr[C=c] = \sum_{m' \in M} Pr[C=c \mid M=m'] \cdot Pr[M=m']$

$= 2^{-\ell} \cdot \sum_{m'} Pr[M=m'] = 2^{-\ell}$ (since $\sum_{m'} Pr[M=m'] = 1$)

$Pr[M=m \mid C=c] = Pr[M=m]$ ← Perfect secrecy

اسمه طول