

Privacy against eavesdroppers

Indistinguishability in the presence of an eavesdropper:

$\text{PrivK}_{\mathcal{A},\Pi}^{\text{eav}}(n)$:

1. \mathcal{A} is given 1^n and outputs m_0 and m_1 such that $|m_0| = |m_1| = \ell(n)$.
2. $k \leftarrow \text{Gen}(1^n)$, $b \leftarrow \{0, 1\}$, and $c \leftarrow \text{Enc}(k, m_b)$.
Then c is given to \mathcal{A} .
3. \mathcal{A} outputs a bit b' .
4. The outcome of the experiment is 1 if $b = b'$ and 0 otherwise.

Definition

A **fixed-length** private-key encryption scheme $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ has indistinguishable encryptions in the presence of an eavesdropper, or is EAV-secure, if for all probabilistic polynomial-time adversaries \mathcal{A} , there is a negligible function negl such that, for all n ,

$$\Pr[\text{PrivK}_{\mathcal{A},\Pi}^{\text{eav}}(n) = 1] \leq 1/2 + \text{negl}(n)$$

Privacy against eavesdroppers

c challenger

Adversary

1^n

m_0, m_1

$K \leftarrow \text{Keygen}$

$b \leftarrow \{0, 1\}$

$\text{Enc}(K, m_b) = c$

c

b'

Adv wins if

$b' = b$

$$\Pr[\text{Adv wins}] = \frac{1}{2} + \text{negl}(n)$$

Multiple message eavesdropping experiment

Challenger

Adversary

$\xrightarrow{1^n}$

$$m_0 = (m_{0,1}, \dots, m_{0,t})$$

$\xleftarrow{\quad} m_1 = (m_{1,1}, \dots, m_{1,t})$

$$|m_{i,0}| = |m_{i,1}| = \ell(n)$$

$$K \leftarrow \text{Keygen}$$

$$b \leftarrow \{0,1\}$$

$$\text{Enc}(K, m_{b,i}) = c_i$$

$\xrightarrow{c_1, \dots, c_t}$

$\xleftarrow{b'}$

Adv wins if

$$b' = b$$

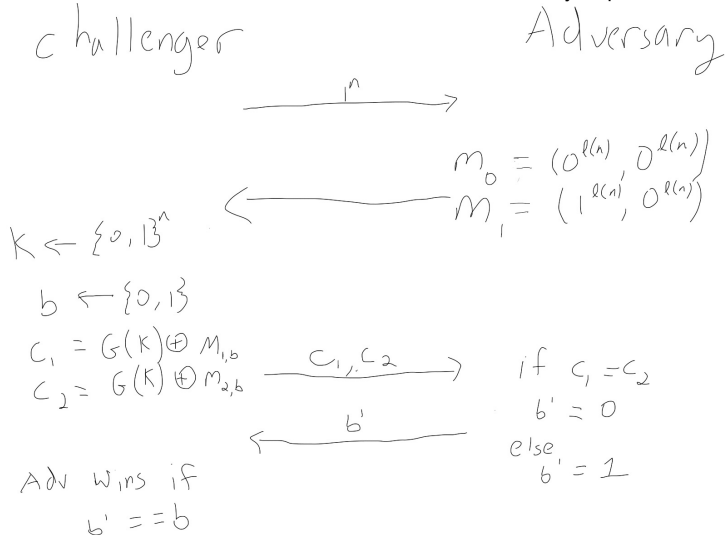
$$\Pr[\text{Adv wins}] = \frac{1}{2} + \text{negl}(n)$$

Pseudo-OTP insecure for multiple messages

Both the OTP and the Pseudo-OTP fail to meet this security requirement.

Pseudo-OTP insecure for multiple messages

Both the OTP and the Pseudo-OTP fail to meet this security requirement.



$$\Pr[\text{Adv wins}] = 1 > \frac{1}{2} + \text{negl}(n)$$