# Symmetric-key encryption scheme.

Alice — Bob

$K$ — $K$

Eve

$Enc(K, M): C \xrightarrow{C} Dec(K, C) = M$

provides confidentiality other than the length of the message

Syntax:

$KeyGen() \to K$

$Enc(K, M) \to C$

$Dec(K, C) \to M$

Correctness: $\forall K, \forall M, C \leftarrow Enc(K, M)$ : $\underline{Dec(K, C) = M}$

Security: Adv
- sees all the algorithms: KeyGen, Enc, Dec
- does not see the randomness used by KeyGen and $K$

Insufficient def: No Adv can reconstruct $M$ from a ciphertext $C$

Broken/Insecure scheme: Adv can tell first letter of $M$, but nothing else

Goal: no partial information about M ~~sta~~ may leak

because Adv can couple it with side information about M & reconstruct M

no Adv should be able to distinguish two messages based on their encryption

Security game: IND-CPA (chosen plaintext attack)

Indistinguishability

Challenger ~~deterministic Enc will be IND-CPA~~ Adv

KeyGen() → K

$\xleftarrow{\quad M \quad}$

$Enc_K(M) = C$ $\xrightarrow{\quad C \quad}$

$\xleftarrow{\quad M_0, M_1 \text{ of the same length} \quad}$

flip a random bit b

$Enc(K, M_b) = C_b$ $\xrightarrow{\quad C_b \quad}$

$\xleftarrow{\quad M' \quad}$

$C' = Enc(K, M')$ $\xrightarrow{\quad C' \quad}$

The bit was b'!

$Enc(K,M) = 2 \cdot M$ × IND-CPA

$Enc(K,M) =$ random number ✓ × correctness

challenge

$Enc(K,M) = K + M \bmod p$

× IND-CPA

$Enc(K,M) = 3$

× correctness

✓ IND-CPA

$\forall$ Adv, $\Pr[\text{Adv wins } (b' = b)] \le 1/2 + negl\left(\frac{1}{2^{128}}\right)$

$2^{128} \gg$ # atoms in the universe

For an IND-CPA + correct scheme, we need

1. One-time pad
2. Block cipher

Alice

$n \rightarrow$ Key size, message size.

KeyGen():

$\boxed{K = k_1, \ldots k_n}$ $\Leftarrow$ chosen randomly

$M = M_1 \ldots M_n$

$Enc(K, M) = K \oplus M$ (bitwise)

$K = 01 \quad M = 11 \Rightarrow C = 01 \oplus 11 = 10$

Bob.

$\boxed{K = K_1 \ldots K_n}$

$Dec(K, C) = K \oplus C$

Correctness:

$Dec(K, C) = K \oplus C =$
$= \cancel{K \oplus} K \oplus M$
$= M$

Is it IND-CPA? NOT IND-CPA

If you use it only $\boxed{\text{once}}$, it is secure.
(one-time)

Claim: Given only one ~~a~~ ciphertext $C$, $(K \,\$ ; C = K \oplus M_b)$

$Pr[Adv(C) = M] \leq negl$; $Pr[Adv(C, M_0, M_1) = M_b] = 1/2$

$K \xleftarrow{\$}$

$$C = M_0 \oplus \underbrace{(M_0 \oplus C)}_{K_0}$$

$$C = M_1 \oplus \underbrace{(M_1 \oplus C)}_{K_1}$$

$K \xleftarrow{\$}$ each is equally likely

! Use one-time pad only once (encrypt only one message per key)