Symmetric-key encryption scheme.

Syntax:

\[ \text{KeyGen()} \rightarrow K \]
\[ \text{Enc}(K, M) \rightarrow C \]
\[ \text{Dec}(K, C) \rightarrow M \]

Correctness: \( \forall K, \forall M, C = \text{Enc}(K, M) : \text{Dec}(K, C) = M \)

Security: \( \text{Adv} \) sees all the algorithms: KeyGen, Enc, Dec

[does not see the randomness used by KeyGen and]

\( K \)

Insufficient def: No \( \text{Adv} \) can reconstruct \( M \) from a ciphered \( C \)

Broken/Insecure scheme: \( \text{Adv} \) can tell first letter of \( M \), but nothing else
Goal: no partial information about $M$ may leak because $\text{Adv}$ can couple it with side information about $M$ & reconstruct $M$.

No $\text{Adv}$ should be able to distinguish two messages based on their chosen plaintext attack.

Security game: $\text{IND-CPA}$

Indistinguishability

Challenger

$\text{Enc}(\cdot)$ will be IND-CA

$\text{Adv}$

$\text{Enc}(K,M) = 2 \cdot M \times \text{Exp}_{\text{CA}}$

Random

$\text{Enc}(K,M) = \text{random number}$

Correctness

$\text{Enc}(K,M) \cdot K + H \mod p$

$\times \text{IND-CPA}$

$\text{Enc}(K,M) = 3$

$\times \text{Correctness}$

$\text{VIND-CPA}$

If $\text{Adv}$,

$\Pr[\text{Adv wins } (b \cdot = b)] = \frac{1}{2} + \text{negl}(\frac{1}{2^n})$ atoms in the universe
For an IND-CPA+ correct scheme, we need

1. One-time pad
2. Block cipher

\[ \text{Alice} \]
\[ n \rightarrow \text{key size, message size} \]
\[ \text{keyGen():} \]
\[ K = k_1 \ldots k_n \quad \leftarrow \text{chosen randomly} \]
\[ M = M_1 \ldots M_n \]
\[ \text{Enc}(K, M) = K \oplus M \quad (bitwise) \]
\[ K = 01 \quad M = 11 \quad \rightarrow C = 01 \oplus 11 = 10 \]

\[ \text{Bob} \]
\[ K = k_1 \ldots k_n \]
\[ \text{Dec}(k, C) = k \oplus C \]

Correctness:
\[ \text{Dec}(K, C) = K \oplus C = K \oplus K \oplus M = M \]

| Is it IND-CPA? | NOT IND-CPA |

If you use it only \( \text{once} \), it is secure.

\( \text{Claim: Given an ciphertext } C, (K \neq M), \frac{\text{Pr}[\text{Adv}(C) = M]}{\text{Pr}[\text{Adv}(C, M_0, M_1) = M_0]} \leq \text{negl}; \text{Pr}[\text{Adv}(C, M_0, M_1) = M_0] \approx \frac{1}{2} \)
\[ K \$
\]
\[ C = M_0 \oplus (M_0 \oplus C) \]
\[ C = M_1 \oplus (M_1 \oplus C) \]
\[ K \$
\]

Each is equally likely.

\[ \square \text{ use one-time pad only once (encrypt only one message per key)} \]