Goal: no partial information about M ~~[illegible]~~ 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

chosen plaintext attack

Security game: IND-CPA

Indistinguishability

Challenger ~~No deterministic Enc will be IND-CPA~~ Adv

KeyGen() → K

← M. ~~[illegible]~~

C ~~[illegible]~~ →

$Enc_K(M)=C$

← M_0, M_1 of the same length — challenge

flip a random bit b

C_b ~~[illegible]~~ →

$Enc(K, M_b)=C_b$

← M'

C' →

$C'=Enc(K,M')$

The bit was b'!

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

2^{128} >> # atoms in the universe

$Enc(K,M)=2 \cdot M$ × IND-CPA

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

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

× IND-CPA

$Enc(K,M)=3$

× correctness

✓ IND-CPA

For an IND-CPA + correct scheme, we need

1. One-time pad
2. Block cipher

Alice

$n \rightarrow$ Key size, message size.

KeyGen():

$\boxed{K = k_1, \dots k_n}$ ← chosen randomly

$M = M_1 \dots M_n$

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

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

Bob

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

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

Correctness:

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

$\boxed{\text{Is it IND-CPA?}}$ NOT IND-CPA

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

Claim: Given $\overset{\text{only one}}{\text{a}}$ 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)