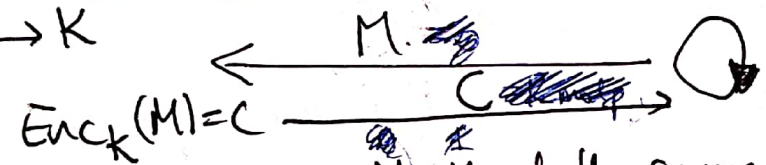


Goal: no partial information about  $M$  ~~also~~ may leak  
 because Adv can couple it with side information about  $M$  & reconstruct  
 no Adv should be able to distinguish two messages based on their encryption

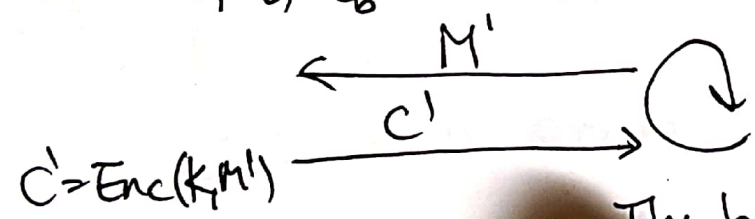
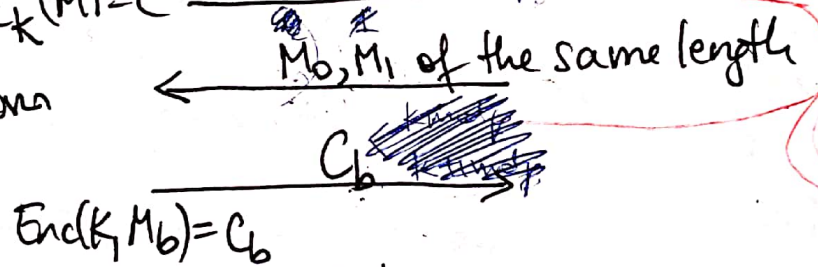
Security game: IND-CPA  
 Indistinguishability  
 — chosen plaintext attack

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

KeyGen()  $\rightarrow$   $K$



flip a random bit  $b$



The bit was  $b'$

$Enc(K, M) = 2 \cdot M$   $\times$  IND-CPA  
 $Enc(K, M) = \text{random number}$   $\checkmark$  correctness

challenge  
 $Enc(K, M) = K \oplus M \text{ mod } p$   
 $\times$  IND-CPA

$Enc(K, M) = 3$   
 $\times$  correctness  
 $\checkmark$  IND-CPA

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

$K = K_1 \dots K_n \leftarrow$  chosen randomly

$M = M_1 \dots M_n$

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

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

Is it IND-CPA? NOT IND-CPA

If you use it only once, it is secure.  
(one-time)

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

$\Pr[\text{Adv}(C) = M] \leq \text{negl}; \Pr[\text{Adv}(C, M_0, M_1) = M_b] =$

$\frac{1}{2}$

Bob

$K = K_1 \dots K_n$

$\text{Dec}(k, c) = k \oplus c$

Correctness:

$\text{Dec}(k, c) = k \oplus c =$   
 $= \cancel{k} \oplus k \oplus M$   
 $= M$

$K \ \$$

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

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

$K \ \$$   
each is  
equally likely

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