OTP has perfect Secrecy

OTP : Encryption $E(k, m) = k \oplus m$

Perfect Secrecy : $\forall m_0, m_1 \in M,\ len(m_0) = len(m_1),\ \forall c \in C$

$$P(E(k, m_0) = c) = P(E(k, m_1) = c)$$

$P(E(K, m_0) = c) \Leftrightarrow$ prob that $\exists$ a key k that encrypts the msg m_0 into c

Think that m_0, c are fixed

$\Updownarrow$

How many keys encrypt m_0 into c with the OTP cipher? ONE!

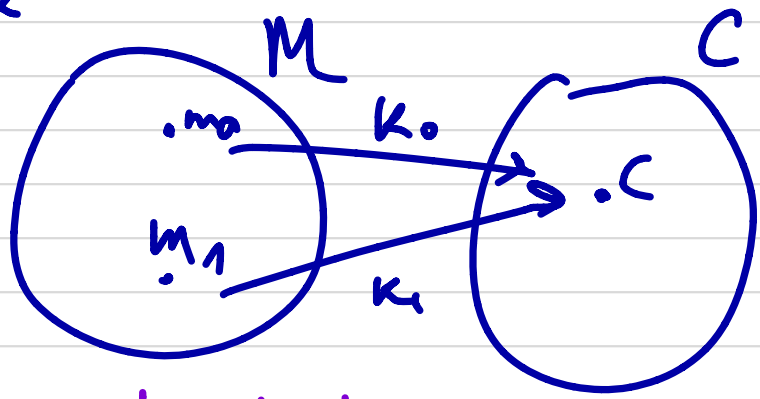
$k \xleftarrow{R} K$

$$P(E_{OTP}(k, m_0) = c) = \frac{\text{How many keys encrypt } m_0 \text{ to } c}{\text{Total number of keys}}$$

$$= 1/|K| = 1/2^n$$

Same reasoning for m_1

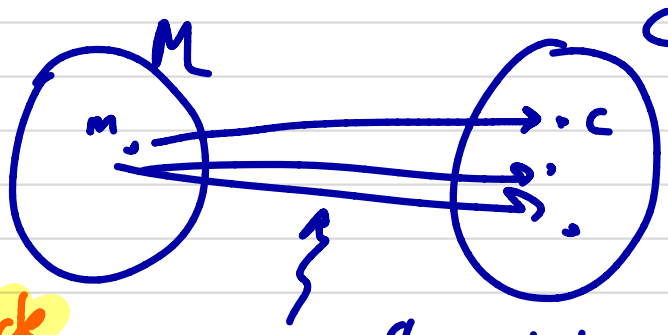
Thus, $P(E(k, m_0) = c) = \frac{1}{2^n} = P(E(k, m_1) = c)$



implication: Perfect Secrecy $\Rightarrow |K| \geq |M|$

Perfect Secrecy $\Rightarrow |K| \geq |M|$

STEP 1 : $|K| \geq |C|$



by def. of Perf. Sec.

$Pr(E(K,m)=c) = \text{constant}$

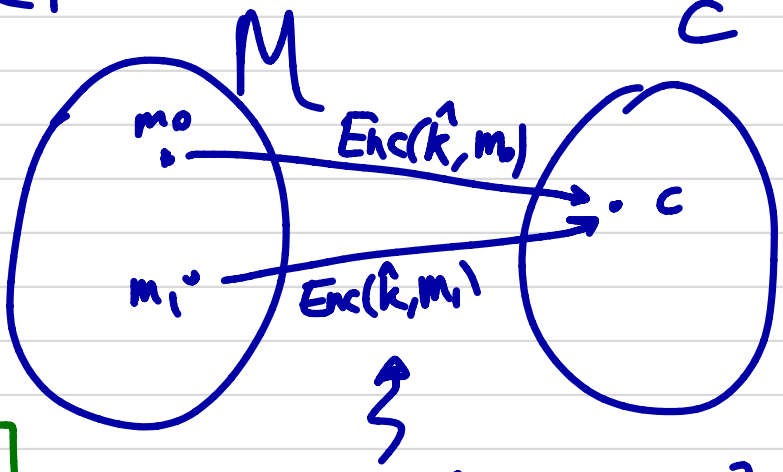
★check pg. 3

all different keys (for different ciphertexts)

$\rightarrow |K| \geq |C|$

STEP 2 $|C| \geq |M|$

By def Encryption is an injective func.



How do I decrypt?

Thus it cannot be $|M| > |C|$

Remark:

$E(K, m_0) = c = E(K, m_1)$

$Prob(\ ) = Prob(\ )$

Perfect Secrecy is asking "how many keys encrypt m_0 to c and m_1 to the same c".

think of k as a variable!

Step 1: for every message m the function $E_m : K \to C$ is surjective $\Rightarrow |K| \geq |C|$

↳ this is true by the def. of Perfect Secrecy

$Prob(E(k,m)=c) = constant > 0$

so fixed a message, there exists at least one key that maps the message into a chosen ciphertext

otherwise it means that $Prob(E(k,m)=c)=0$ $\forall m, \forall c$ → there is no encryption

⟹ check the additional material for detailed proofs