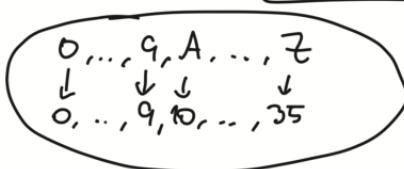


OTP $(\text{Gen}, \text{Enc}, \text{Dec})$

$$\Sigma = \{0, \dots, 9, A, \dots, Z\}$$

$$M = \Sigma^7$$

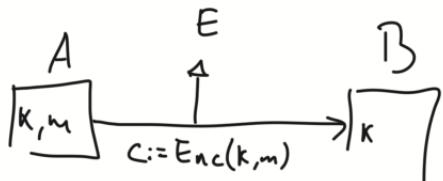
$$K = M$$



$K = A$	F	1	C	B	Z	4
10	15	1	12	11	35	4
$m =$	1	C	3	2	5	3
18	18	12	3	2	5	3
$m+k =$	28	33	13	15	13	7

$$C := \text{Enc}(k, m) = \underline{\begin{matrix} 5 & w & D & F & D & 4 & 7 \end{matrix}}$$

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



Perfect secrecy:

$\forall c \in C, m_1, m_2 \in M$, ocurre que:

$$\Pr_{k \leftarrow K} [\text{Enc}(k, m_1) = c] = \Pr_{k \leftarrow K} [\text{Enc}(k, m_2) = c]$$

Teorema (Shannon, 1949)

Un sistema criptográfico simétrico ($\text{Gen}, \text{Enc}, \text{Dec}$) puede tener perfect secrecy sólo si $|M| \leq |K|$.

Dem: Por contradicción sup. $|M| > |K|$ y perf. sec.

Sea $m_0 \in M$ y $k_0 \in K$, $c_0 := \text{Enc}(k_0, m_0)$

$$S := \{m \in M \mid \exists k \in K \text{ } \text{Enc}(k, m) = c_0\}$$

Queda pendiente para la próxima clase...

Teorema: OTP tiene perfect secrecy

$c_0 \in C \quad m_0 \in M$

$$\Pr_{k \in K} [Enc(k, m_0) = c_0] \text{ von OTP}$$

$$\Pr_{k \in K} [k + m_0 = c_0]$$

$k + m_0 = c_0$ sólo ocurre para $k = c_0 - m_0$

$$\text{por lo tanto } \Pr_{k \in K} [Enc(k, m_0) = c_0] = \frac{1}{|K|}$$

$\Rightarrow \forall m_1, m_2 \in M \quad c_0 \in C$

$$\Pr_{k \in K} [Enc(k, m_1) = c_0] = \frac{1}{|K|} = \Pr_{k \in K} [Enc(k, m_2) = c_0]$$

$m = 1 \quad 1 \quad C$

$K = A \quad F \quad 1$

$\Sigma = \{0, 1\}$

m en ASCII es 01101001 0101001 01100011

A F 1

01100001 01100110 00110001

$c = Enc(k, m) = m \oplus k = 00000100000001110101010$

OTP es seguro frente a un atacante que ve el texto cifrado, pero no seguro frente a uno que puede ver el texto plano.

Suponiendo que una llave se usa una sola vez

$$C_0 := M_0 \oplus K \quad C_1 := M_1 \oplus K$$

$$\underline{C_0 \oplus C_1} = (M_0 \oplus K) \oplus (K \oplus M_1) = M_0 \oplus (\cancel{K \oplus K}) \oplus M_1 \\ = \underline{M_0 \oplus M_1}$$

El atacante sí gana información si se usa la misma llave más de una vez.