One Time Pad (OTP) -

$$m \oplus k \rightarrow c$$

Encryption: $c = k \oplus m$
Decryption: $m = k \oplus c$

$\oplus$ (XOR)	k: 0	k: 1
$m(c)$: 0	0	1
$m(c)$: 1	1	0

The key k:

- is as long as the plaintext m and the ciphertext c
- is uniformly random chosen in $\mathcal{K}$
- must be used only once

Perfect Secrecy

For all m possible plaintext (i.e., all m in $\mathcal{M}$) and any c ciphertext (i.e., all c in $\mathcal{C}$) such that $Pr[C=c]>0$, it holds:

$$Pr[M=m|C=c] = Pr[M=m]$$

Theorem (key length bounding):

Let (Enc, Dec) be a perfectly-secret encryption scheme over a plaintext space $\mathcal{M}$ and a key space $\mathcal{K}$. Then it holds that $|\mathcal{K}| \geqslant |\mathcal{M}|$ (i.e., the length of the key is larger or equal to the length of the message).

Examples

$$\begin{array}{rl} k: & 0\,1\,1\,0\,1\,1\,0\,0 \;\oplus \\ m: & 1\,0\,1\,1\,1\,0\,0\,1 \\ \hline c: & 1\,1\,0\,1\,0\,1\,0\,1 \end{array}$$

$$\begin{array}{rl} k: & \mathtt{G\ F\ N\ O\ M} \;\oplus \\ m: & \mathtt{P\ A\ G\ E\ S} \;(\text{mod } 26) \\ \hline c: & \mathtt{V\ F\ T\ S\ E} \end{array}$$

\+ Easy, fast encryption and decryption

− Long key length

Multiple use of the same key k

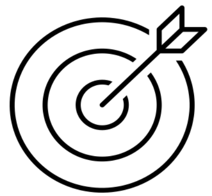
$c_1 = k \oplus m_1,\ c_2 = k \oplus m_2, \ldots$

Attack 1. $\mathcal{A}$ knows the ciphertexts c_1, c_2

$\mathcal{A}$ finds a relation between the plaintexts: $m_1 \oplus m_2 = c_1 \oplus c_2$

Attack 2: $\mathcal{A}$ knows (at least) the pair (m_1, c_1)

$\mathcal{A}$ finds the key $k = m_1 \oplus c_1$, then decrypts $m_2 = k \oplus c_2$



Perfect secrecy

Pages on SecuRity
by Ruxandra F. Olimid