



Perfect secrecy

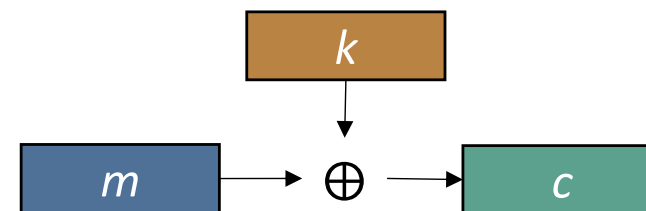
The key k :

- is as long as the plaintext m and the ciphertext c
- is uniformly random chosen in \mathcal{K}

Vernam Cipher (1917)

Encryption: $c = k \oplus m$

Decryption: $m = k \oplus c$



10

$$\begin{array}{r} k: 0\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ \oplus \\ m: 1\ 0\ 1\ 1\ 1\ 0\ 0\ 1 \\ \hline c: 1\ 1\ 0\ 1\ 0\ 1\ 0\ 1 \end{array}$$

$$\begin{array}{r} k: B\ V\ Q\ G\ F\ B\ \oplus \\ m: N\ O\ T\ I\ M\ E\ (\text{mod } 26) \\ \hline c: O\ J\ J\ O\ R\ F \end{array}$$

Multiple use of the same key k

$$c_1 = k \oplus m_1, c_2 = k \oplus m_2, c_3 = k \oplus m_3, \dots$$

1. **Ciphertext-only attack:** \mathcal{A} just observes the ciphertexts

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

2. **Known-plaintext attack:** \mathcal{A} knows (at least) one pair (m_1, c_1) encrypted with k

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

3. **Chosen-plaintext attack (CPA):** \mathcal{A} can obtain the encryption of a plaintext of his/her choice

4. **Chosen-ciphertext attack (CCA):** \mathcal{A} can obtain the decryption of a ciphertext of his/her choice

For 3 and 4, \mathcal{A} can apply the same attack from 2.