XOR Cipher (a.k.a Vernham Cipher)

a modern version of Vigenere

Use ⊕ to combine the message and the key

$$E_k(m) = k \oplus m$$

$$D_k(c) = k \oplus c$$

$$D_k(E_k(m)) = k \oplus (k \oplus m) = m$$

Problem : known-plaintext attack

so $k = (k \oplus m) \oplus m$

$$x \oplus x = 0$$

$$x \oplus 0 = x$$

Mauborgne Cipher - a modern version of OTP

Use a random stream as encryption key

➡ Defeats the know-plaintext attack

Problem : Key-reused attack (a.k.a two-time pad)

$$C_1 = k \oplus m_1$$
$$C_2 = k \oplus m_2$$
$$\text{so } C_1 \oplus C_2 = (k \oplus m_1) \oplus (k \oplus m_2)$$
$$= (m_1 \oplus m_2) \oplus 0$$
$$= (m_1 \oplus m_2)$$

$$x \oplus x = 0$$
$$x \oplus 0 = x$$