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)

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

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

The impossibility of breaking OTP

The ciphertext bears no statistical relationship to the plaintext

➡ No statistical analysis

For any plaintext and ciphertext, there exists a key mapping one to the other, and all keys are equally probable

➡ A ciphertext can be decrypted to any plaintext of the same length