

# OTP - One Time Pad

➔ Improvement over Vigenere cipher

**Algorithm :** combine the message and the key

**Key :** an infinite random string

**Key space :** infinite

	whatanicedaytoday
⊕	yksuftgoarfwfwel
	<hr/>
	ZZZJUCLUDTUNNWGQS

**Advantage :** **this is the perfect cipher !**

**Disadvantage :** hard to use in practice, how to transmit the key ?

# XOR Cipher (a.k.a Vernham Cipher)

a modern version of Vigenere

**Use**  $\oplus$  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

$$\text{so } k = (k \oplus m) \oplus m$$

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