OTP

Message = P Key = k

$C = P \oplus k$

length (P) = length (K)

→ Key must be private, random and used only once

Symmetric cryptography

→ The same key to encode and to decode (the two parties have the same key)
→ needs to be shared before

Asymmetric cryptography

→ 2 Keys (public, private)
→ public key encrypt
→ private key decrypt

RSA

p, q → prime numbers

$n = p \cdot q$ $\Phi(n) = (p-1)(q-1)$

e → int factor of n

Public key → (n, e)

$d = \frac{k\,\Phi(n) + 1}{e}$ $\quad k \rightarrow$ a random value

Private key → (n, d)

Encrypt : $C = M^e \bmod n$ (M : message)

Decrypt → $M = C^d \bmod n$

OTP Quantum

$X|0\rangle = |1\rangle \qquad X|M\rangle = |M \oplus 1\rangle$
$X|1\rangle = |0\rangle$

$|E\rangle = X_k |M\rangle$ → apply X if $k = 1$

$X|+\rangle = |+\rangle \qquad Z|0\rangle = |0\rangle$
$X|-\rangle = -|-\rangle \qquad Z|1\rangle = -|1\rangle$

$Z|+\rangle = |-\rangle$
$Z|-\rangle = |+\rangle$

X basis $|E\rangle = Z_{k_2} X_{k_1} |M\rangle$ → Encrypt

$|D\rangle = X_{k_1} Z_{k_2} |E\rangle$ → Decrypt

⇒ To use the X basis, in this case, you first encode the message in the Z basis, then apply $H^{\otimes n}$, and finally add the key using X gate.