Quantum cryptography: BB84 protocol

Giulia Di Gregorio

First year PhD seminar

Outline

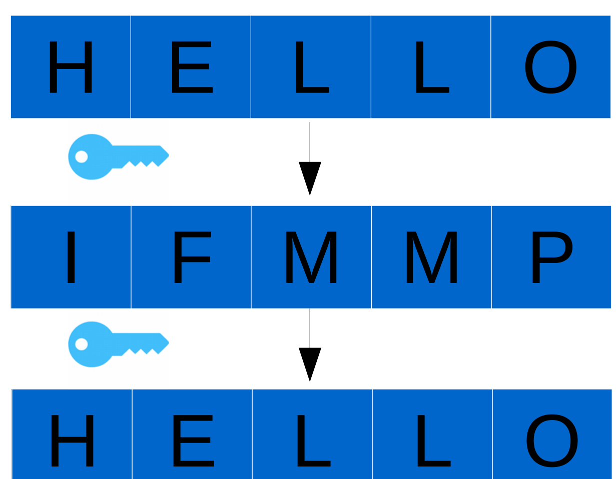
- Basics of cryptography
- Problem of classical cryptography
- Quantum cryptography
- BB84 protocol
- Experimental results & conclusions

What is cryptography?

- Cryptography is the study of techniques for secure communication in presence of third parties (eavesdroppers).
- A cryptographic scheme has 5 ingredients:
  - Plain text;
  - Encryption algorithm;
  - Key;
  - Cipher text;
  - Decryption algorithm.

Vocabulary

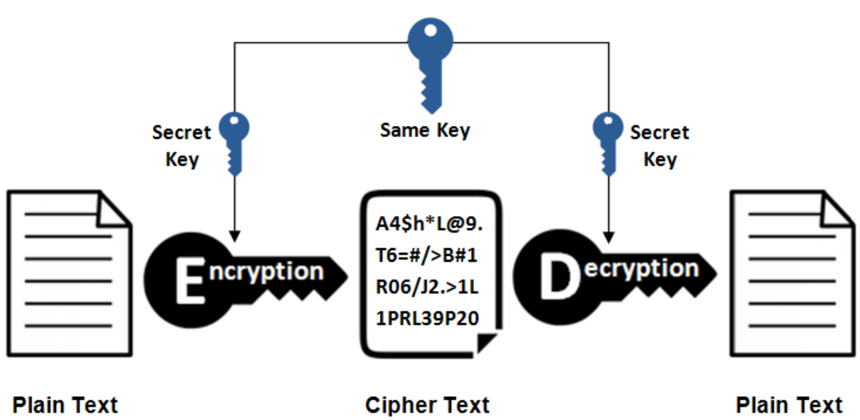
- Plain text: data to protect during the transmission.
- Encryption algorithm: algorithm used to encrypt the plain text.
- Key: code used to encrypt the message.
- Cipher text: encrypted message.
- Decryption algorithm: algorithm used to decrypt the cipher text.



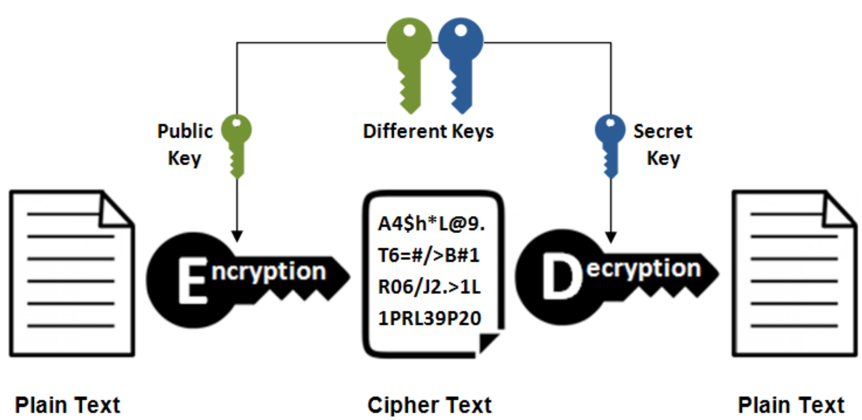
Types of cryptosystems

- Symmetric key cryptography (theoretically secure)
  - Same key for encryption and decryption;
  - Secret key.
- Asymmetric key cryptography (not secure → chosen plain-text attack):
  - Separate key for encryption and decryption;
  - Public key for encryption;
  - Private key for decryption.

Symmetric Encryption



Asymmetric Encryption

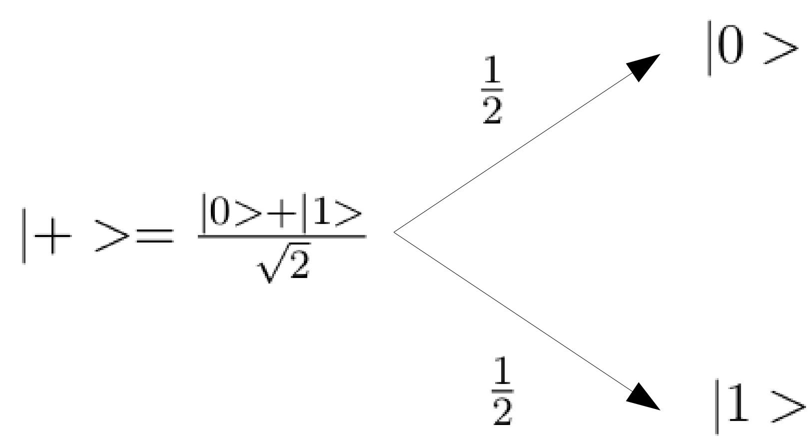


Problem

- How to exchange the secret key?

Quantum cryptography

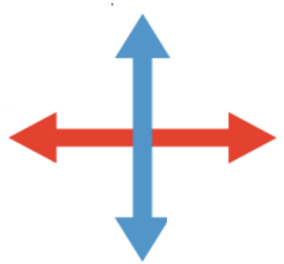
- Quantum cryptography solves the problem of the key distribution.
- Any third party, who performs measurements, will be discovered.
- <u>Key points</u>:
  - No-cloning theorem;
  - Quantum superposition.



BB84 protocol

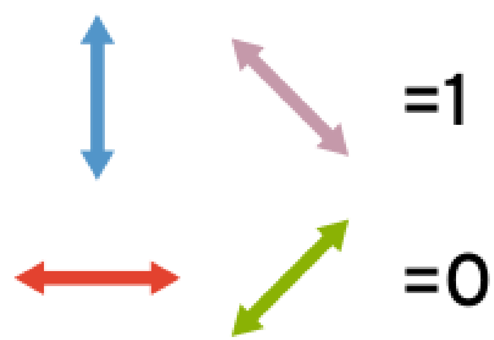
- Protocol that allows two people to share a private key [1].
- The protocol uses polarized photons.

Rectilinear basis



Diagonal basis

- Each photon polarization represents a bit.



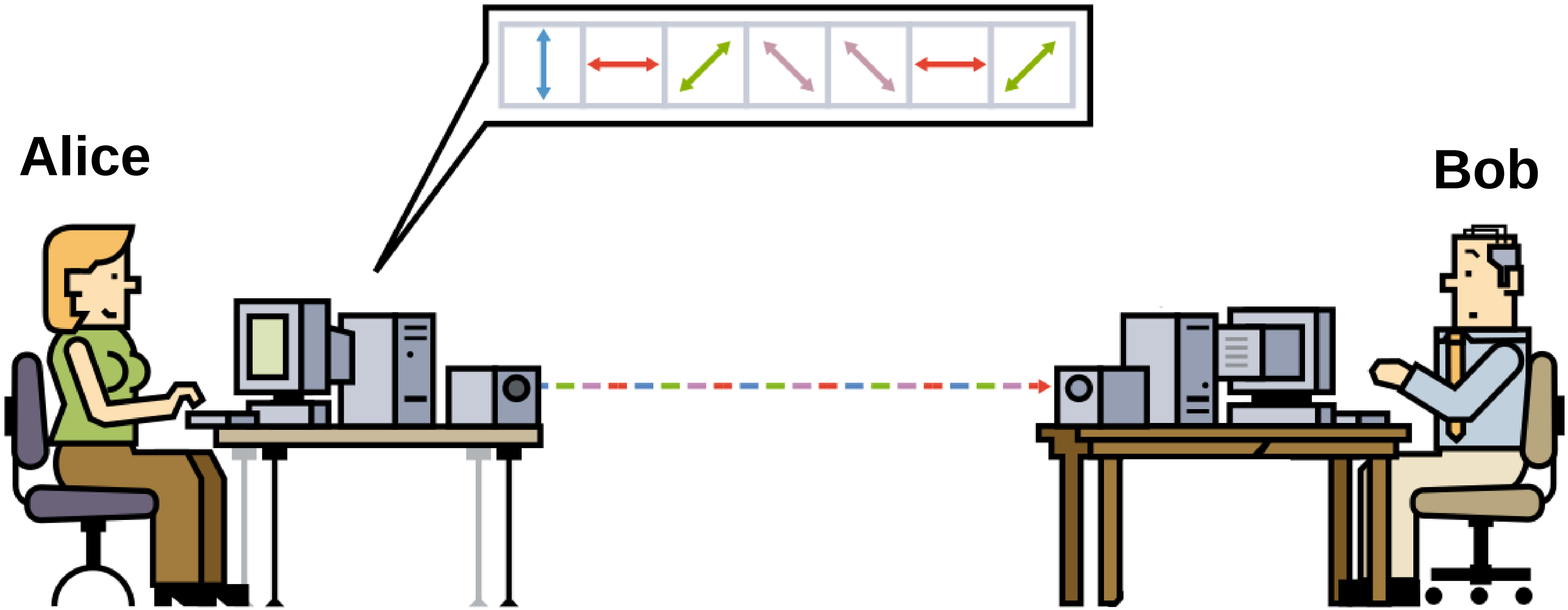
- The two parties have access to one classical channel and one quantum channel.

Example

Alice

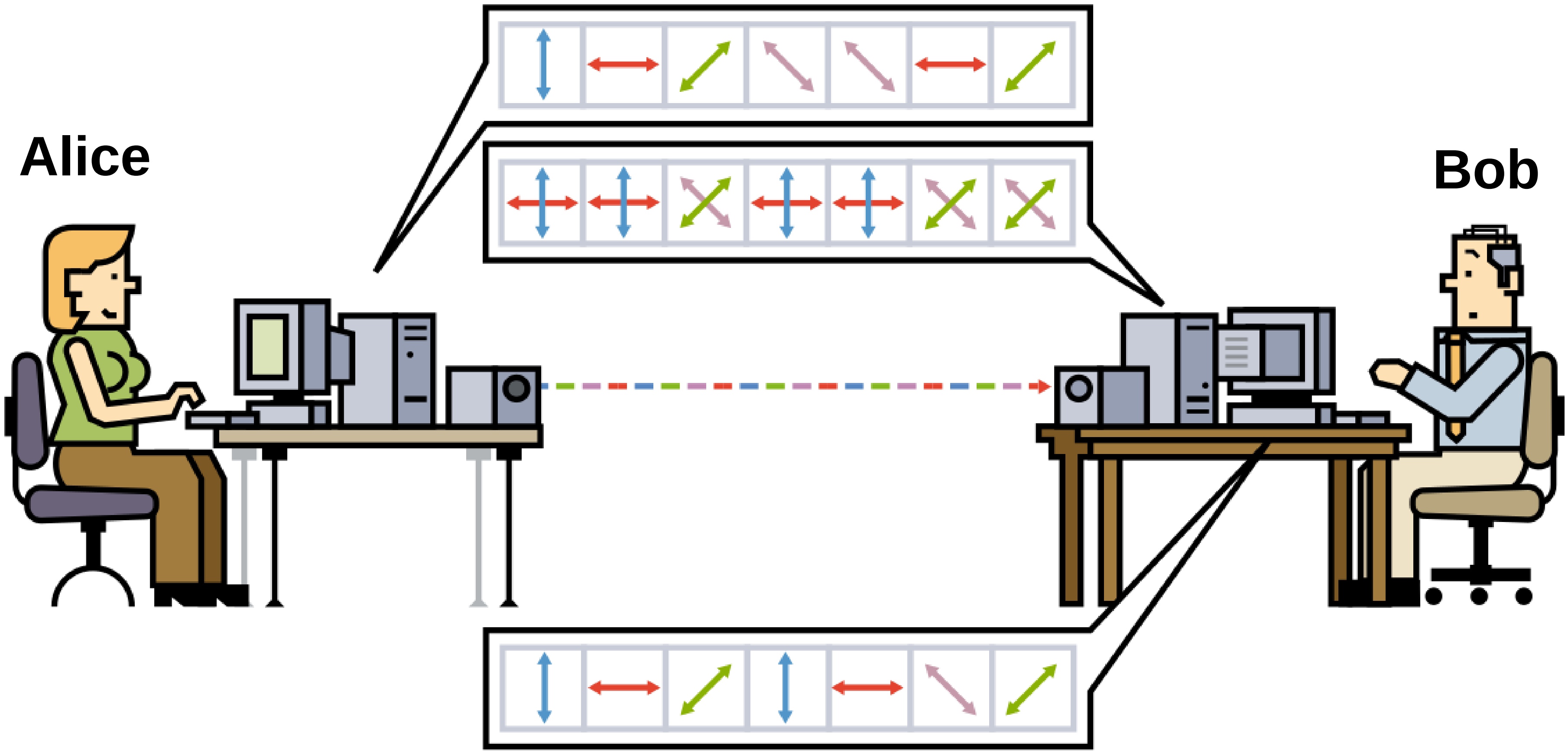
Bob

Example



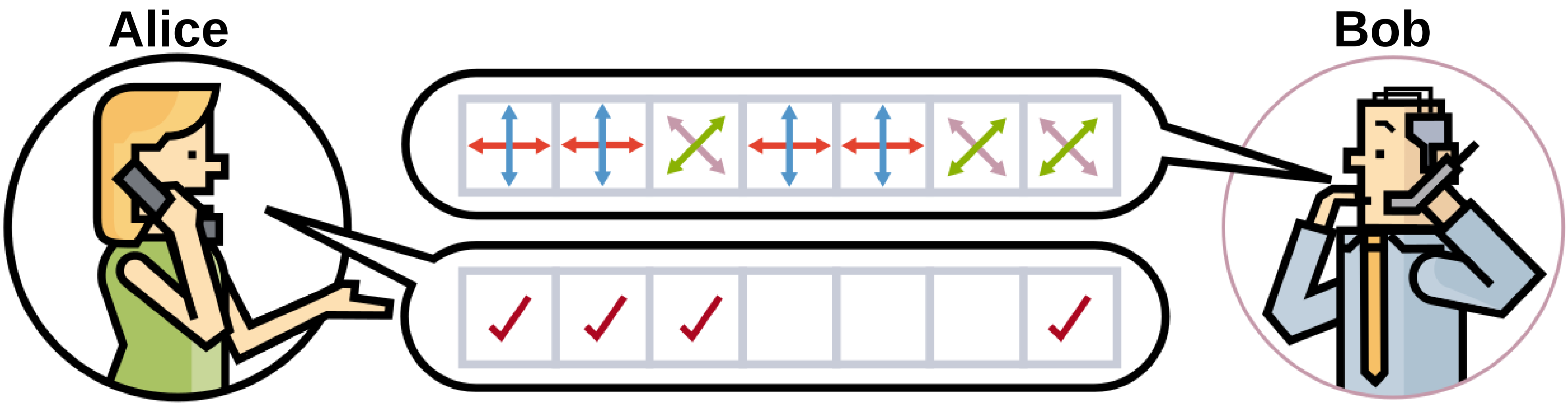
- Alice chooses **randomly** the polarization of each photon sent to Bob.

Example



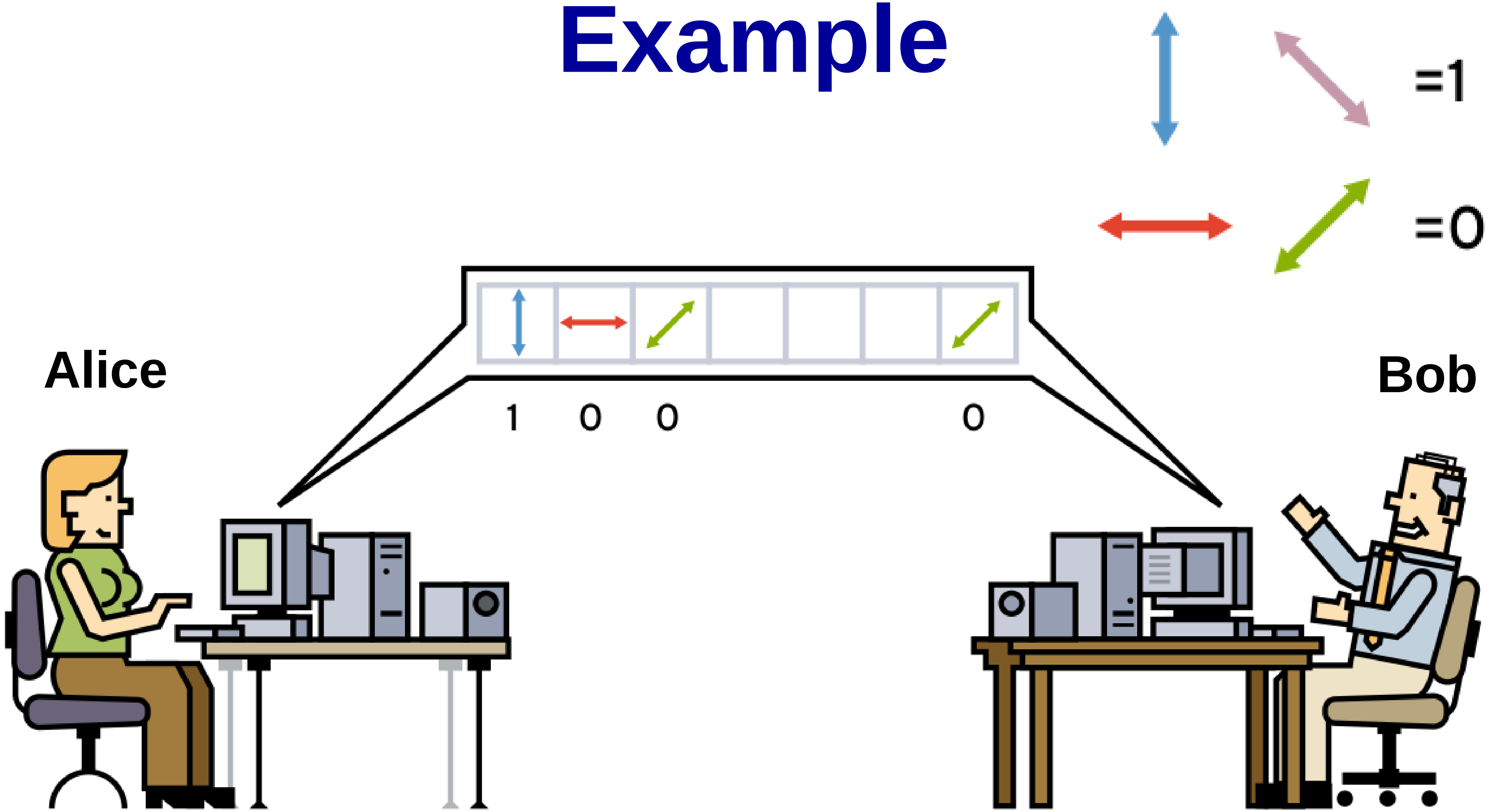
- Alice chooses **randomly** the polarization of each photon sent to Bob.
- Bob chooses **randomly** one of the basis for each photon and measures their polarization.

Example



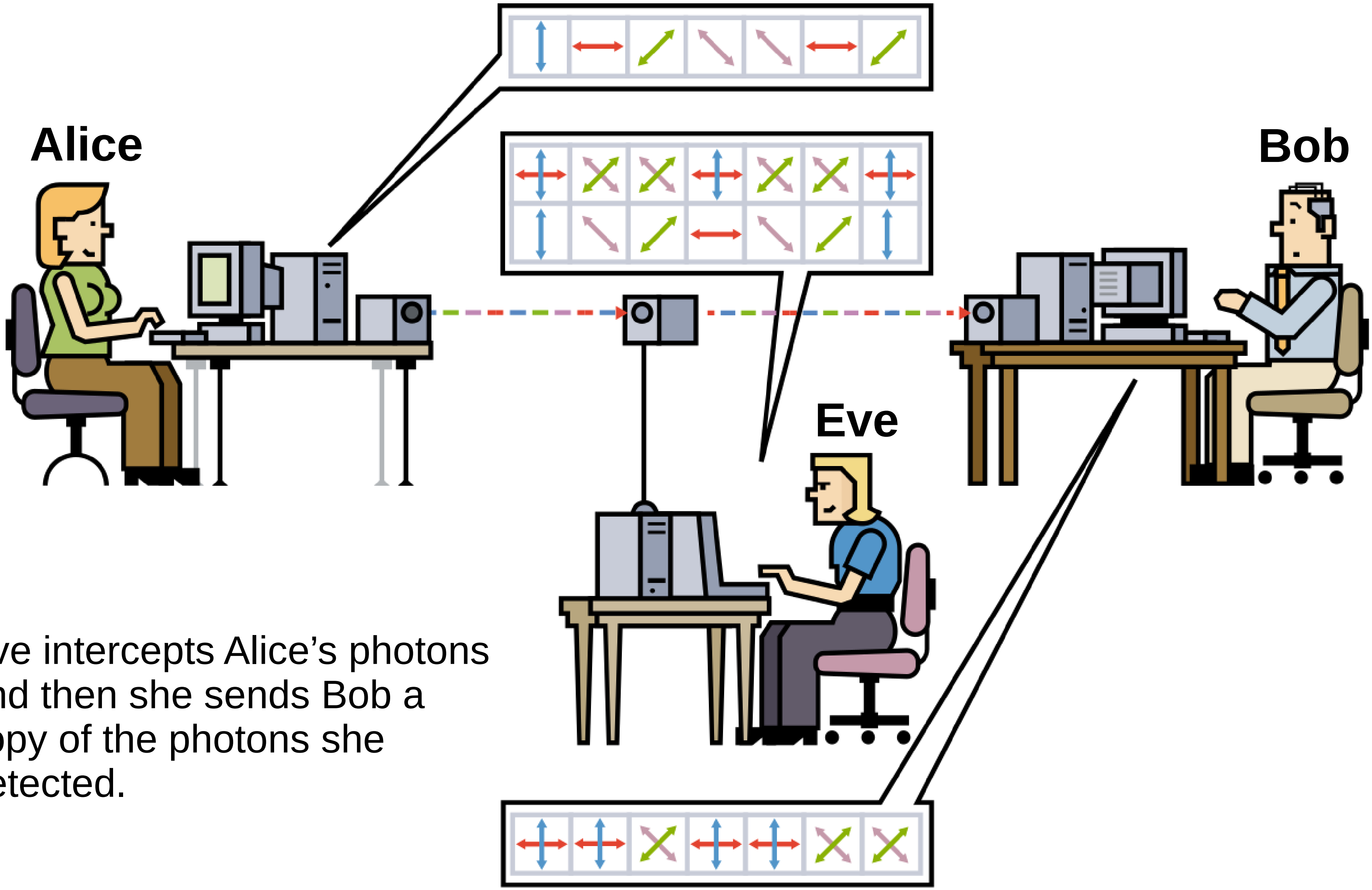
- Using the classical channel, Bob announces which basis he used.
- Alice replies if his choices were correct.

Example



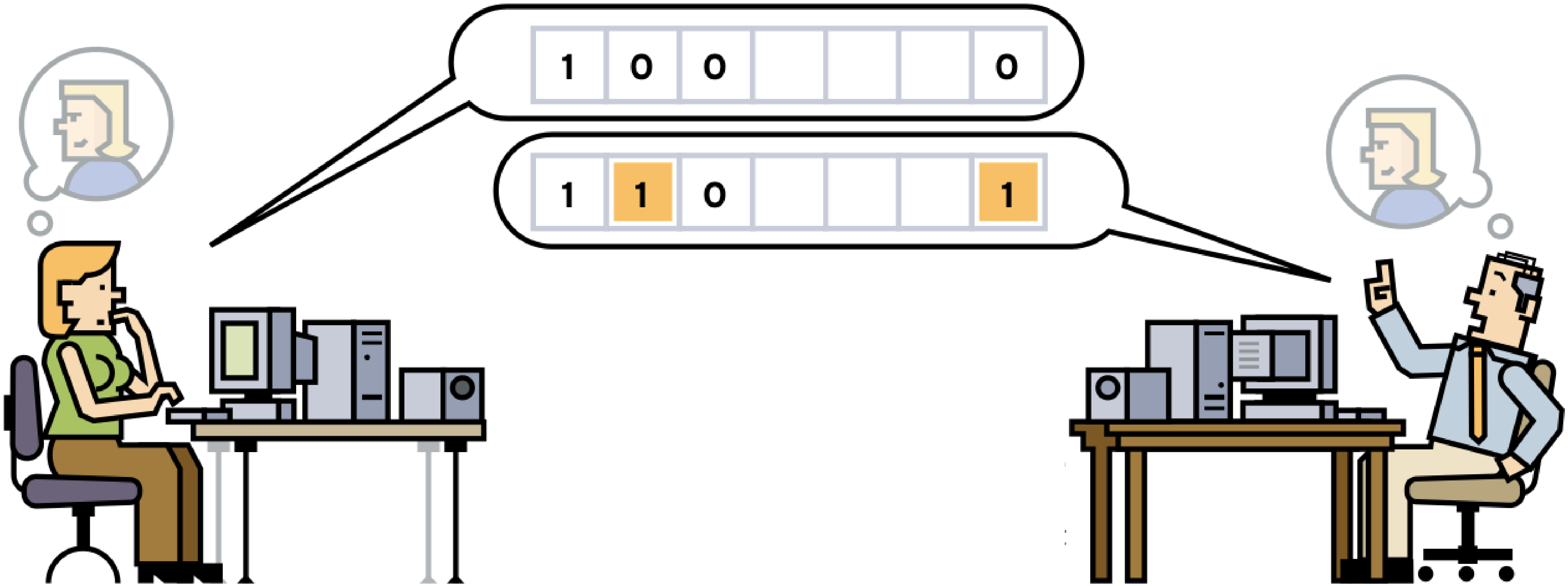
- Alice and Bob keep only the bits corresponding to the correct basis.

How to foil eavesdropper



- Eve intercepts Alice’s photons and then she sends Bob a copy of the photons she detected.

How to foil eavesdropper (2)



- Alice and Bob reveal some bits to cross-check only for the matching basis.

Experimental results & conclusion

<u>Problems:</u>

- No single photon source → weak laser pulses.
- No single photon detection → avalanche photodiodes.
- Transmission of the light → optical fibers.

<u>Successes:</u>

- Transmission using optical fiber to distance of ~ 400 km [2].
- Open air transmission to distance of ~ 140 km [3].

<u>Conclusions:</u>

- Quantum cryptography is a major achievement in secure engineering.
- It solves the problem of key distribution between the parties.

BACK UP SLIDES

References

[1] Bennett, C. & Brassard, G. “Quantum cryptography: Public Key Distribution and coin-tossing.”, *IEEE Int. Conf. on Computers Systems and Signal Processing* (1984) vol 175.

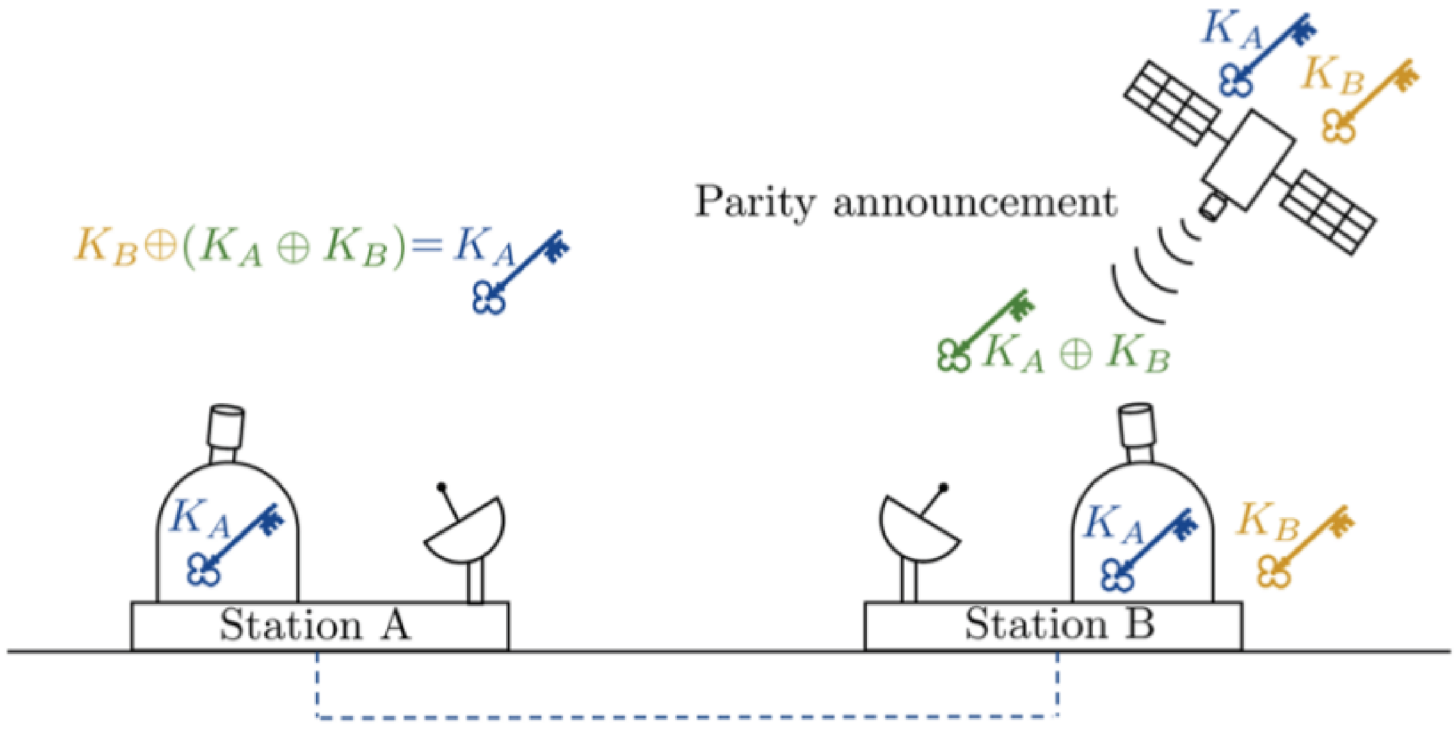
[2] Yin, H. *et al.* “Measurement device independent quantum key distribution over 404 km optical fibre.”, *Phys. Rev. Lett.* (2016) 117.

[3] Ursin, R. *et al.* “Free-space distribution of entanglement and single photons over 144 km.” *Nat. Phys.* (2007) vol 3.

[4] Yin, J. *et al.* “Satellite-based entanglement distribution over 1200 km.”, *Science* (2017) vol 365.

QKD via satellite

- It is possible to exchange the key via low orbit satellites [4].
- The satellite holds all keys.
- Each time that A and B want to communicate, satellite sends the XOR of the two key (K_A XOR K_B).



One Time Pad (OTP)

- It is a perfect cipher that it cannot be cracked.
- Weakness:
  - The secret key must be as long as the message it's intended to encrypt.
  - A copy of the key must somehow be distributed to the receiver.

ENCRYPTION

```
      H       E       L       L       O  message
   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) message
+ 23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= 30      16      13      21      25     message + key
=  4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) (message + key) mod 26
      E       Q       N       V       Z  → ciphertext
```

DENCRYPTION

```
      E       Q       N       V       Z  ciphertext
   4 (E)  16 (Q)  13 (N)  21 (V)  25 (Z) ciphertext
-  23 (X)  12 (M)   2 (C)  10 (K)  11 (L) key
= -19      4      11      11      14     ciphertext – key
=   7 (H)   4 (E)  11 (L)  11 (L)  14 (O) ciphertext – key (mod 26)
      H       E       L       L       O  → message
```

RSA

- RSA is one of the asymmetric cryptosystems.
- It is based on the practical difficulty of the factorization of the product of two large prime numbers.
- Step:
  - Choose two integer prime numbers p and q.
  - Compute $n = pq$ and $f(n) = (p-1)(q-1)$.
  - Choose e such that $1 < e < f(n)$ and e and $f(n)$ coprime.
  - Determine d such that $de = 1 \ (mod\ f(n))$
  - e is the public key
  - d is the private key

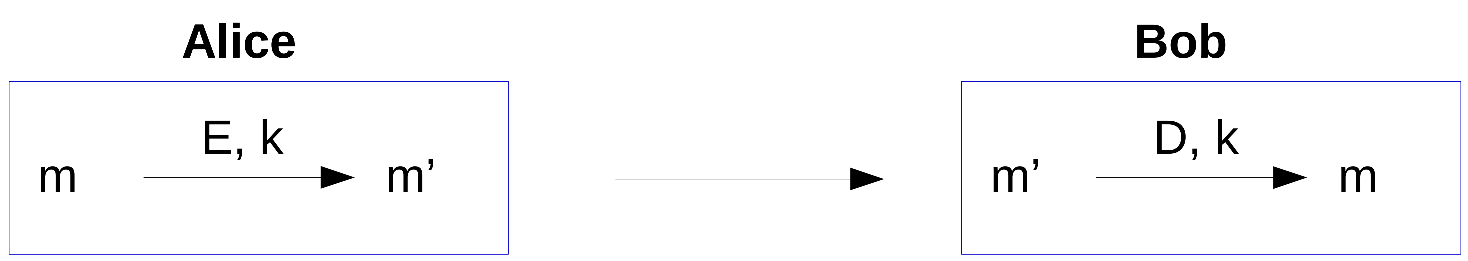
Symmetric-key encryption

- It is an encryption method in which both the sender and the receiver share the same key *k.*

  m = message to send

  m' = E(m, k) = encrypted message

  D(m', k) = D(E(m, k), k) = m



Asymmetric-key encryption

- It is an encryption process where different key are used for encrypting and decrypting.
- The keys are different but mathematically related.

PROS	CONS
• If there are *n* user, the total number of key is *2n* (in symmetric algorithms *n(n-1)/2*). • Not required a secure channel for the initial exchange.	• Slower than symmetric algorithms. • The system can be attacked by chosen-plain text attack.

No-cloning theorem

There is no unitary transformation *U* such that, for any state $|\psi>$:

$$U |\psi>|0> = |\psi> |\psi>$$

<u>Proof</u>: taken two states $|\psi_1>$ and $|\psi_2>$, we have:

$$U |\psi_1>|0> = |\psi_1>|\psi_1>$$

$$U|\psi_2>|0> = |\psi_2>|\psi_2>$$

Since *U* is unitary, the scalar product remains unchanged:

$$<\psi_2|\psi_1> = <\psi_2|\psi_1>^2$$

This means that:

- it is possible to clone a state if we know it or if we know its orthogonal states;
- it is impossible to clone unknown states.