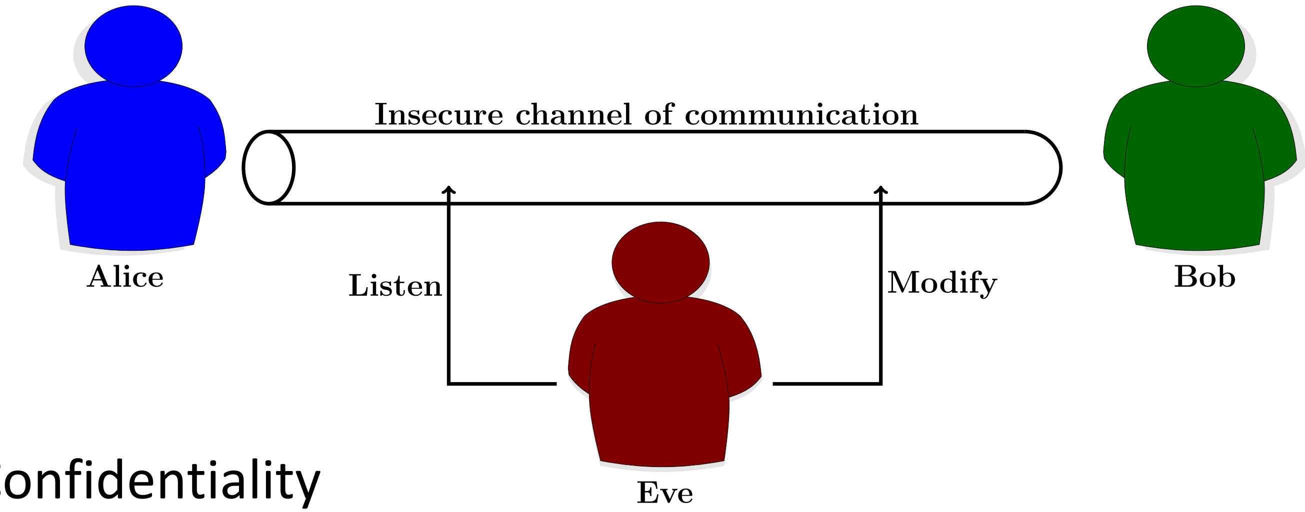
Introduction
to
Public-Key Cryptography

Cryptography: four directions



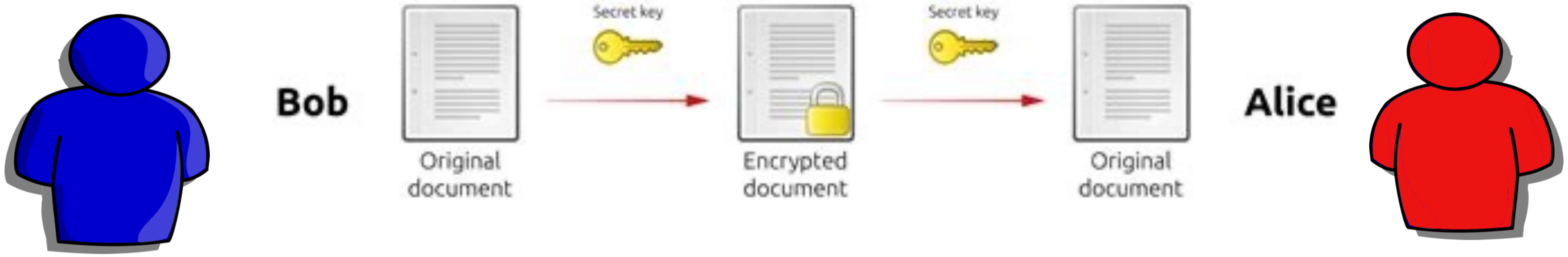
- Confidentiality
- Message Integrity
- Sender Authentication
- (soft) Sender Undeniability (non-repudiation)

Kerckhoffs' Principle

- A cryptographic system should be secure even if everything about the system, except the key, is public knowledge.
- Modern Applications demand even Tamper-Resistance

Pic credits: wikipedia.org

Symmetric Key Cryptography



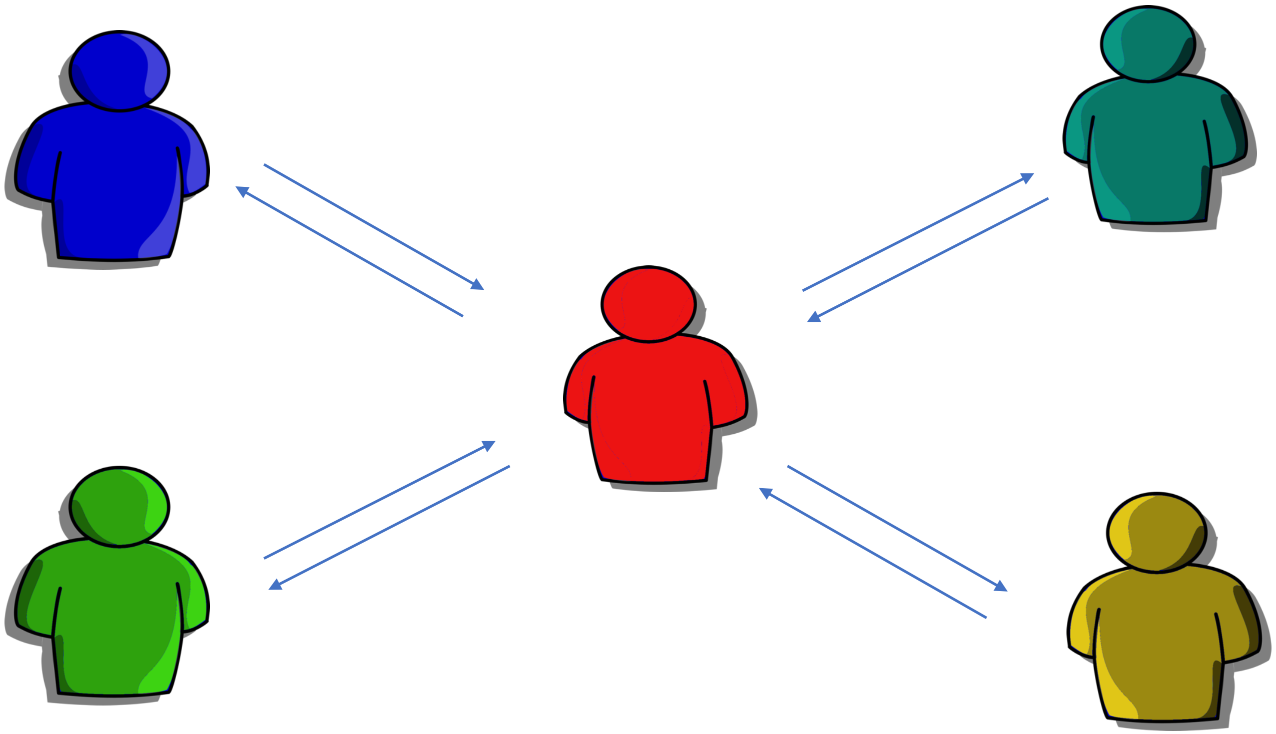
The keys for encryption and decryption are identical

Question: How to have the shared secret key?

Pic credits:commons.Wikimedia.org, openclipart.org

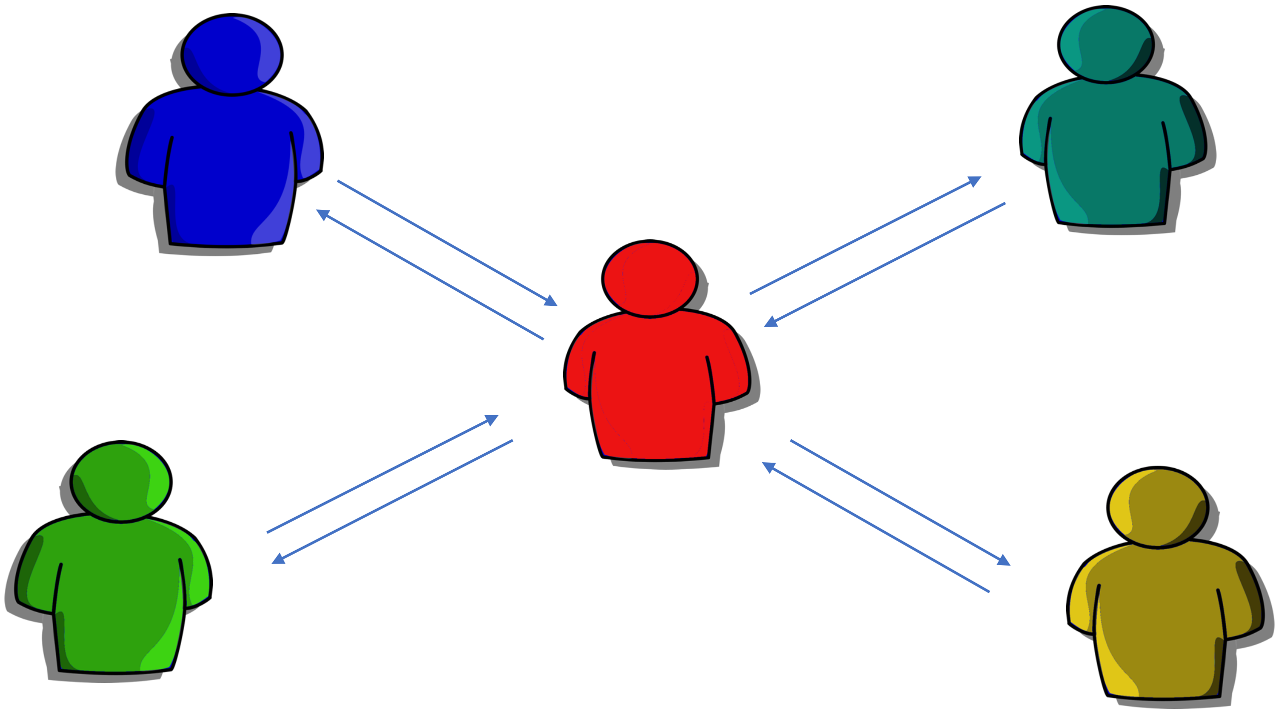
The main bottleneck

- Each pair needs a separate key



The main bottleneck: Key management

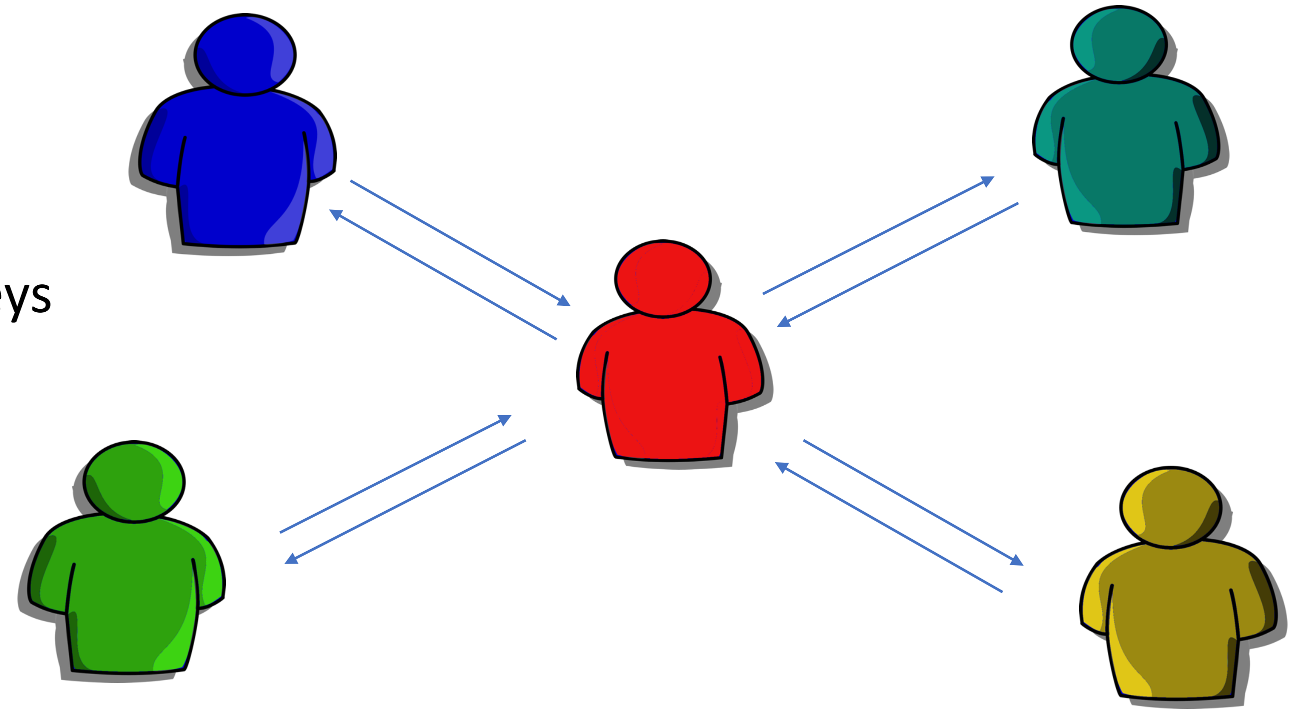
Everyone needs (n-1) many different keys: one for each other person.



The main bottleneck: Key management

Everyone needs (n-1) many different keys: one for each other person.

Total n(n-1)/2 many keys

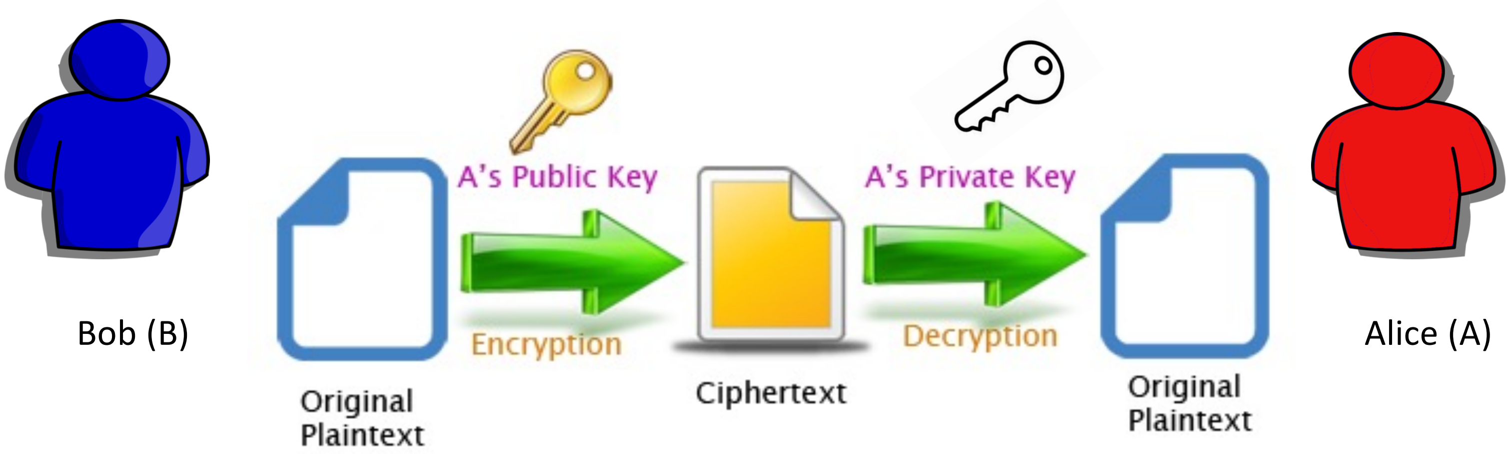


Can we reduce the number of keys

Public Key Cryptography

- Each person has two keys: one public and one Private
- The keys are asymmetric: Related but not identical
- Public Key is known to everyone, private key is kept secret

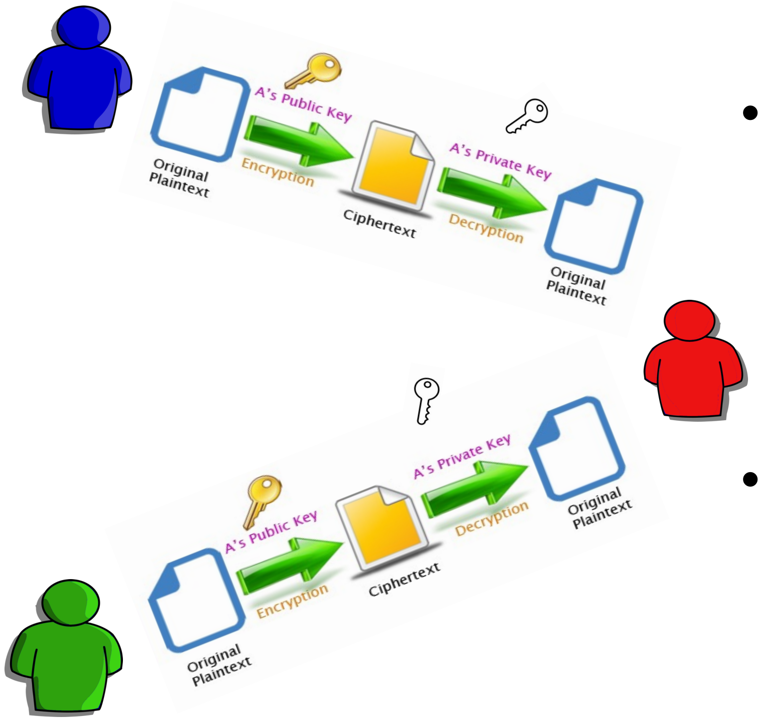
Public Key Encryption



Take home: Encryption using receiver's public key, decryption using receiver's secret key.

Pic credits: flaticon.com, http://www.giuseppeurso.eu,openclipart.org

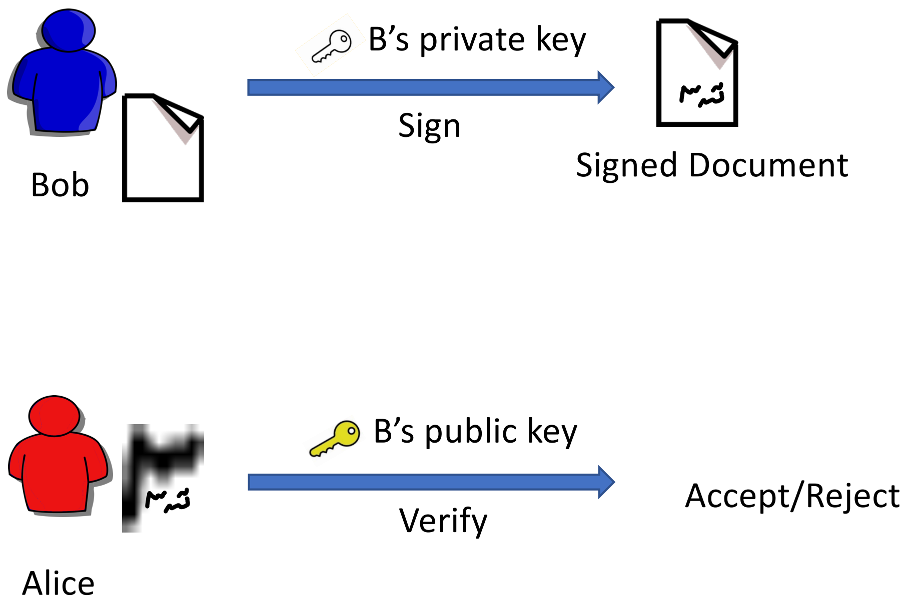
Public Key Encryption (Key Management)



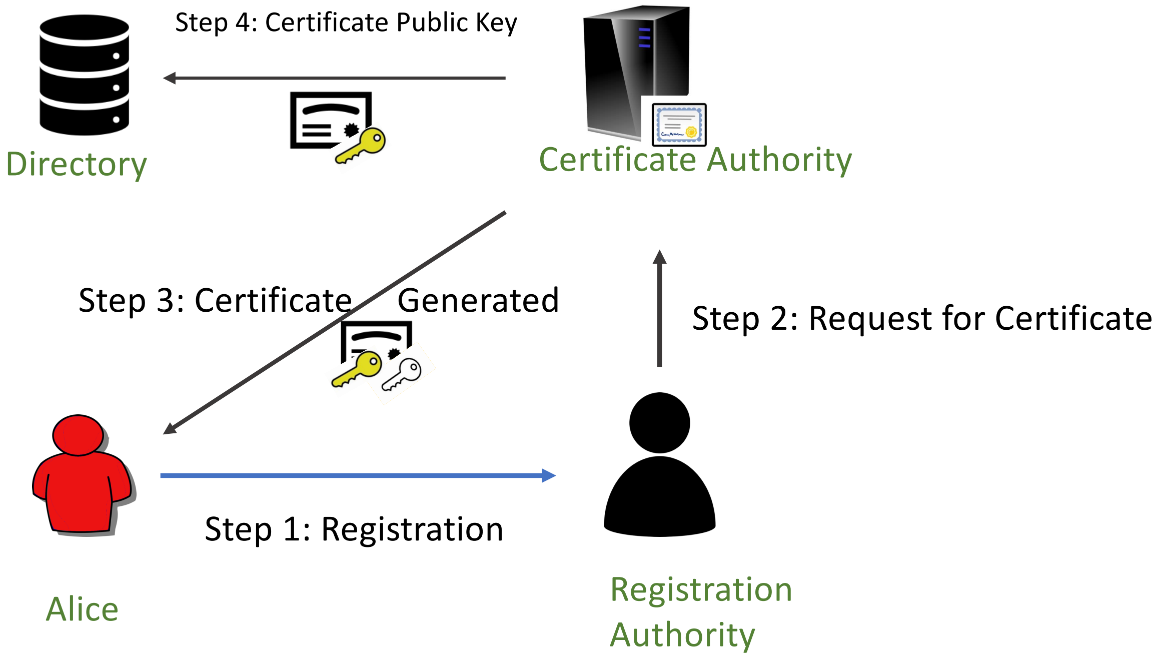
- We no longer need pairwise distinct keys
- For secret communication among n people, we need n secret keys and corresponding n public keys

Pic credits: flaticon.com, http://www.giuseppeurso.eu,openclipart.org

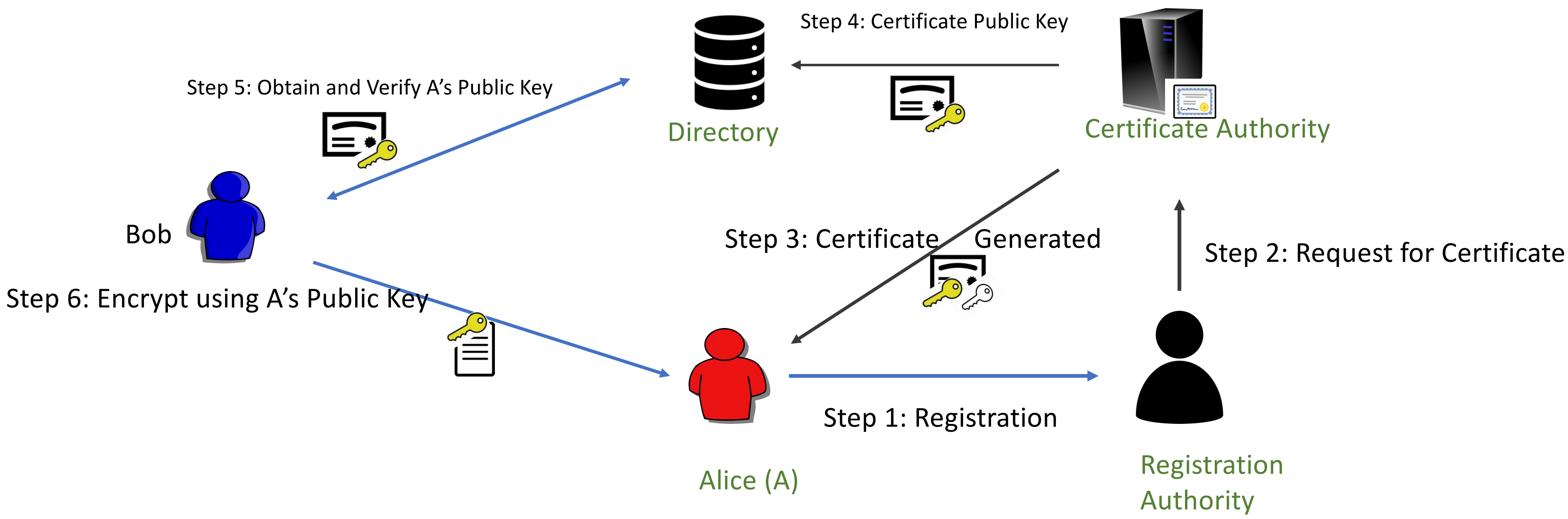
Public Key Authentication: Signatures



Public Key Infrastructure



Public Key Infrastructure




THANK
YOU