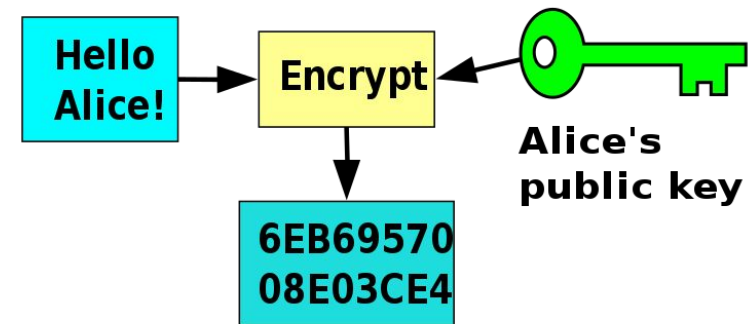


Asymmetric Encryption

- **Public-key cryptography**, or asymmetric cryptography, is a cryptographic system that uses pairs of keys: public keys which are made public, and private keys which are known only to the owner.
- **Data encrypted with the private key can only be decrypted with the public key, and vice versa.**
- In such a system, any person can encrypt a message using the receiver's public key, but that encrypted message can only be decrypted with the receiver's private key.

Bob



Alice

