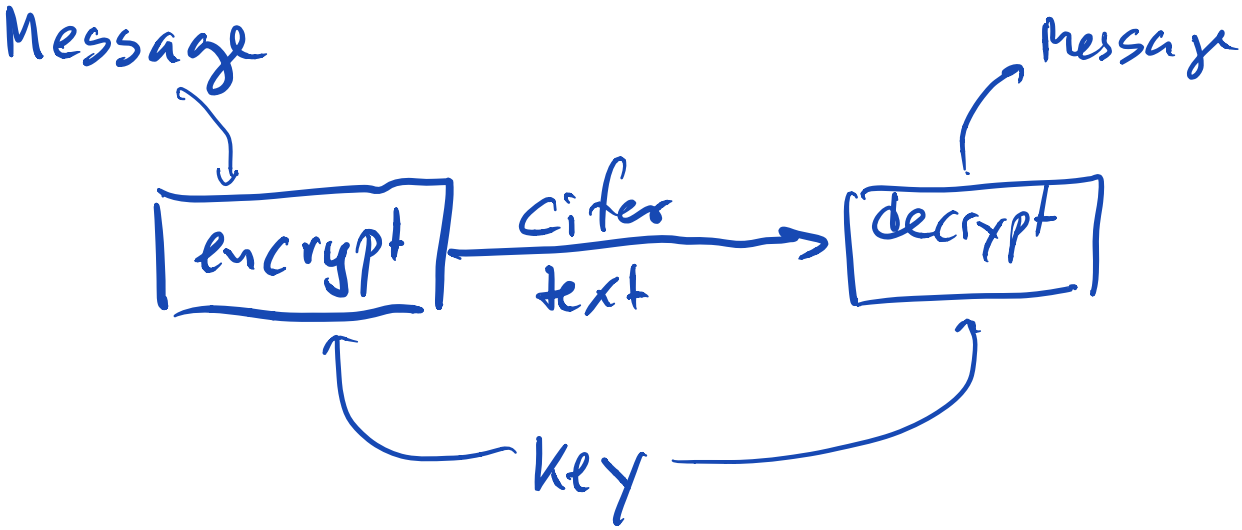
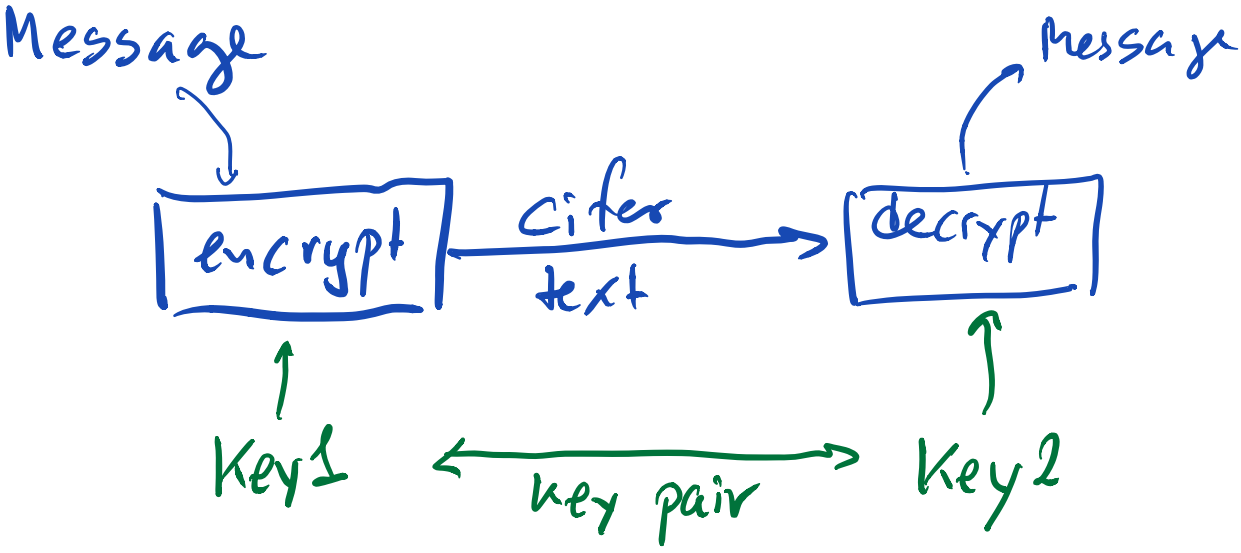
Symetric Encryption



How to get to aggree on a key?

Asymetric encryption



2 scenarios

- A and B work together to create a key pair (possible, but not done in our usecase)
- A create a keypair and keeps key1 secret, and key2 public ✓

Asymetric key encryption scenarios

- Signing
- Encrypting
- Signed encryption
- Certificates

Asymetric encryption under the hood

The basic idea is that

- Message is a very big number (byte array)
- It is hard to find the factors in a large number
  - → see wikepedia on Division algorithm

⟹ ((Show RSA code))

Exercises

- Change from encrypt scenario to sighing
- Extend to "Sign & encrypt"

Diffie Hellman Merkle key exchange

public

$(Y \hat{} X) \% P$

$Y = 23$

$P = 117$

A pick $X = 17$

B pick $X = 7$

((Show code))

$$K_b = ((Y \hat{} X_a) \% P) \hat{} X_b \% P$$

$$= (Y \hat{} X_a \hat{} X_b) \% P$$

$$K_a = ((Y \hat{} X_b) \% P) \hat{} X_a \% P$$

$$= (Y \hat{} X_b \hat{} X_a) \% P$$

Exercise: change code such that

- Uses big random primes
- A and B exchange a secret using AES

Most public / asymetric alg says

"pick a huge random prime"

What if they are not random

SecureRandom instead of Random