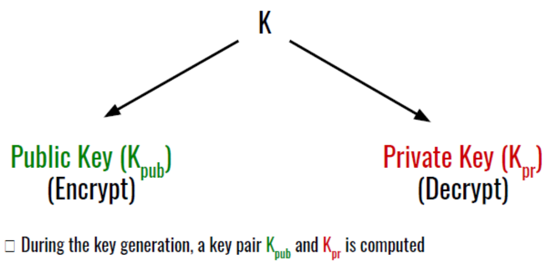
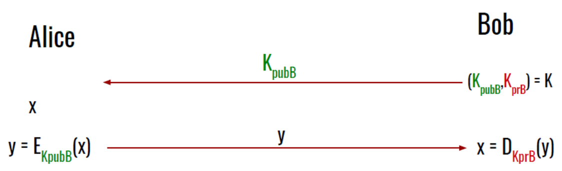
4. Asymmetric ciphers


K
Public Key (K_{pub})
(Encrypt)
Private Key (K_{pr})
(Decrypt)
□ During the key generation, a key pair K_{pub} and K_{pr} is computed

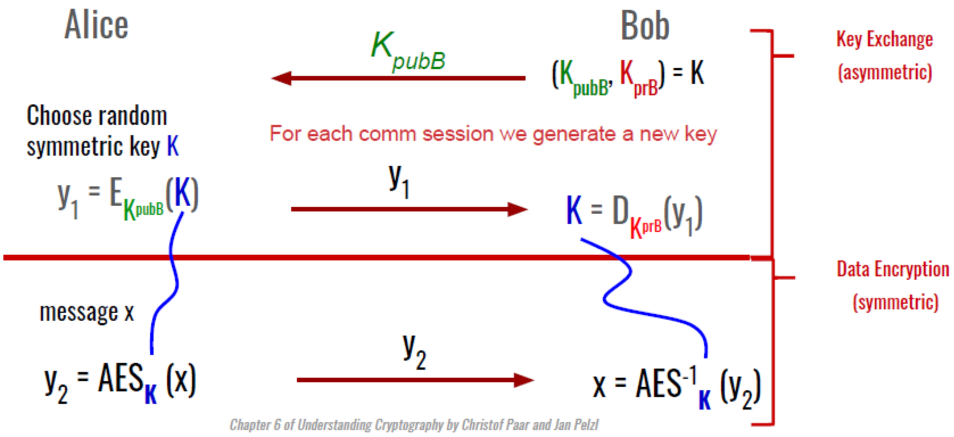


Main mechanisms:

- **Key Distribution** without a pre-shared secret (key)
- **Nonrepudiation and Digital Signatures** (e.g., RSA, DSA or ECDSA)
- **Identification:** using challenge-response protocols with digital signatures
- **Encryption** (e.g., RSA / Elgamal) Disadvantage: Complex in computation

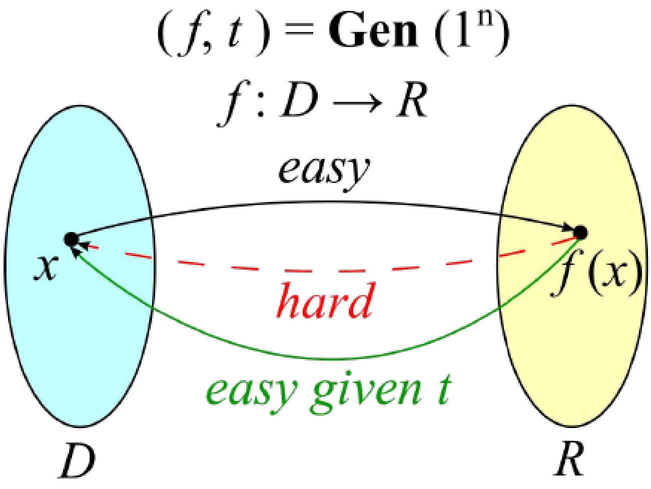
Hybrid system: mix symmetric and asymmetric

1. Key exchange with slow asymmetric
2. Encryption of data with fast symmetric ciphers



Chapter 6 of Understanding Cryptography by Christof Paar and Jan Pelzl

To build PK schemes we can use One Way Function (OWF):



t stays for **trapdoor**

There is no proof that OWFs actually exists. However, there are a few good candidates (no one proved yet they are not one way):

- **[IF] integer factorization** with prime numbers:
  f(x) = p * q where p and q are prime numbers is easy to compute
  given f(x) is hard to perform factorization to get p and q
- **[DL] discrete logarithm:**
  f(x) = ab mod p where is p is prime is easy to compute
  given f(x) is hard to compute b = log a f(x)
- **[ECC] Elliptic Curves:** based on elliptic curve discrete logarithm problem

FOCUS ON RSA