# Other asymmetric cryptography schemes

**Diffie-Hellman** (precursor)

➡ No Authentication but good for key-exchange

**El-Gamal**

➡ Good properties for homomorphic encryption

**Elliptic Curve Cryptography** (widely used nowadays)

➡ Fast and small keys (190 bits equivalent to 1024 bits RSA)

# Asymmetric vs Symmetric

| | Symmetric | Asymmetric |
|---|---|---|
| pro | Fast | No key agreement |
| cons | Key agreement | Very slow |

The best of both worlds

- Use RSA to encrypt a shared key
- Use AES to encrypt message

$$E_{Kp}(m) = RSA_{Kp}(k), AES_k(m)$$

Naive approach