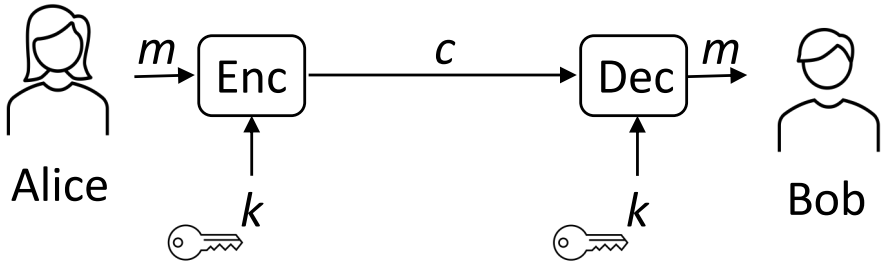
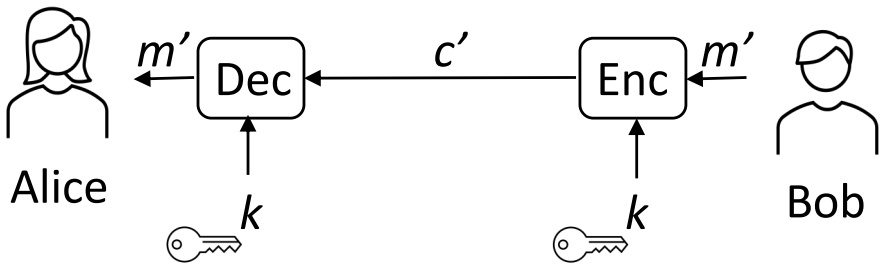
Symmetric vs. Asymmetric Encryption -

Symmetric	Asymmetric

... encryption

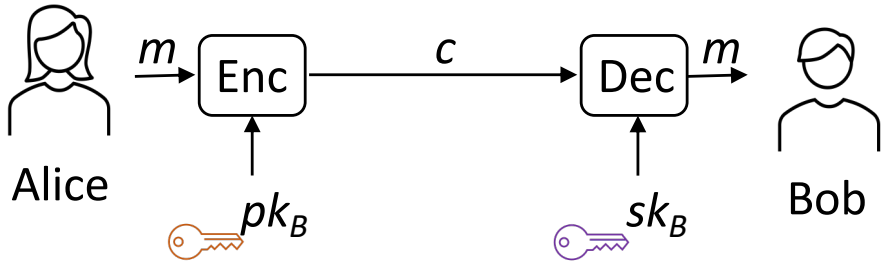


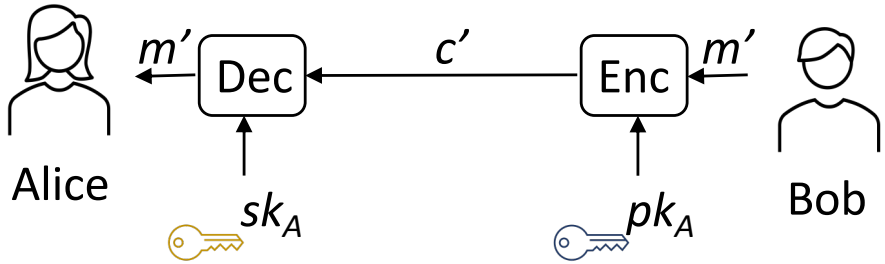


Encryption: $c = \text{Enc}(k,m)$
Decryption: $m=\text{Dec}(k,c)$
Correctness: $\forall m \in \mathcal{M}, k \in \mathcal{K}$
$\text{Dec}(k,\text{Enc}(k,m)) = m$

Shorter keys (+)

Key establishment (−)





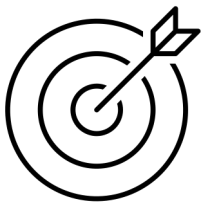
(+) Private keys never leave the owner

(−) Computational cost & speed

Encryption: $c = \text{Enc}(pk_B,m)$
Decryption: $m=\text{Dec}(sk_B,c)$
Correctness: $\forall m \in \mathcal{M}, (pk_B, sk_B) \in \mathcal{K}$
$\text{Dec}(sk_B,\text{Enc}(pk_B,m)) = m$

Terminology

k: symmetric key
pk: public key
sk: private (secret) key
(pk,sk): public-private key pair
m: plaintext
c: ciphertext
Enc: encryption alg.
Dec: decryption alg.
Cryptanalysis



Confidentiality

No. of keys

for N bi-directional communicating parties

Each: N-1 [k]	vs.	*Each: 1 [sk], N-1 [pk]*
Total: N(N-1)/2 [k]		*Total: N [sk], N [pk]*