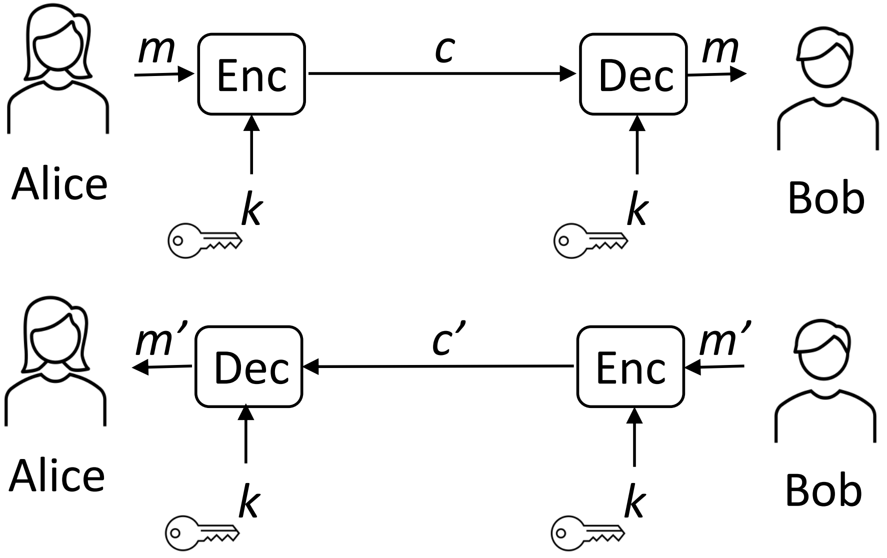
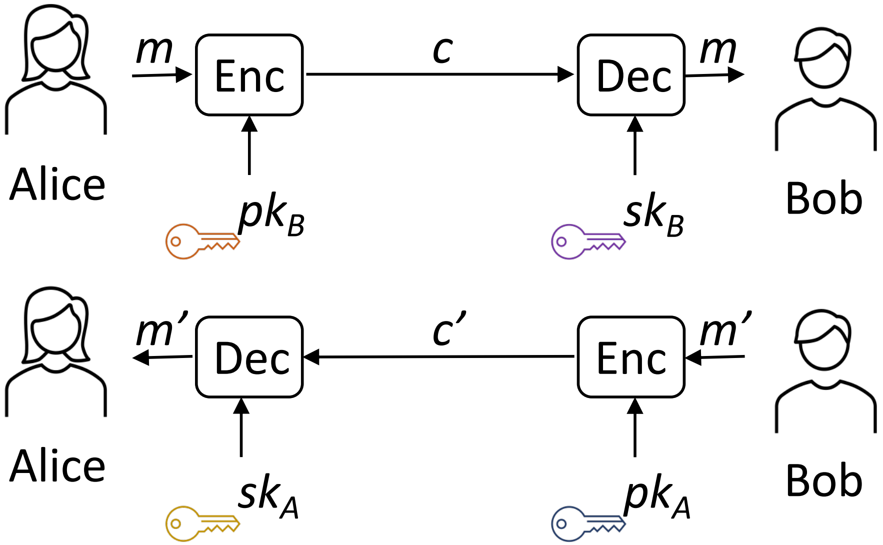
Symmetric vs. Asymmetric Encryption -

www.ruxandraolimid.weebly.com/pagesonsecurity

Symmetric | Asymmetric

… encryption





Encryption: $c = \mathrm{Enc}(k,m)$
Decryption: $m=\mathrm{Dec}(k,c)$
Correctness:
$\mathrm{Dec}(k,\mathrm{Enc}(k,m)) = m$

Shorter keys +

Key distribution −

+ Private keys never leave the owner

− Computational cost & speed

Encryption: $c = \mathrm{Enc}(pk_B,m)$
Decryption: $m=\mathrm{Dec}(sk_B,c)$
Correctness:
$\mathrm{Dec}(sk_B,\mathrm{Enc}(pk_B,m)) = m$

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]*

Pages on SecuRity
by Ruxandra F. Olimid