Asymmetric encryption for **confidentiality**

Bob encrypts a message $\mathbf{m}$ with Alice's public key $\mathbf{Kp}_{\mathrm{A}}$

➡ Nobody can decrypt $\mathbf{m}$, except Alice with her private key $\mathbf{Ks}_{\mathrm{A}}$

✓ Confidentiality without the need to exchange a secret key

K_{sA}, K_{pA}

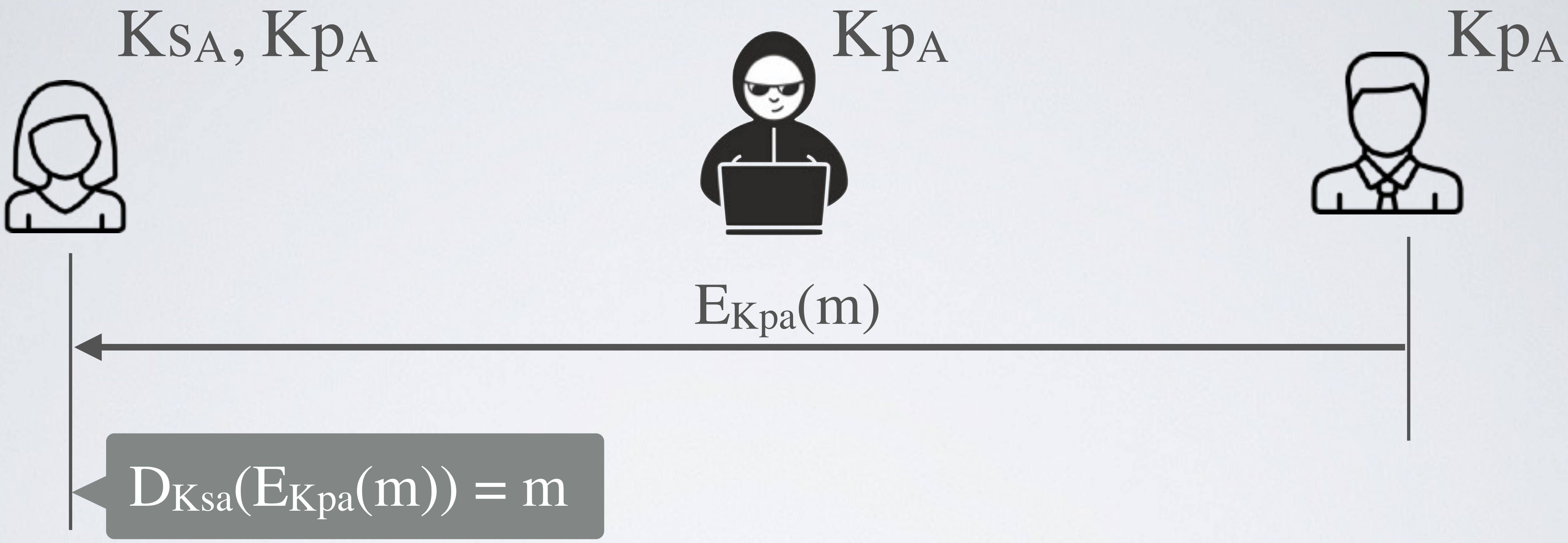
Kp_A

Kp_A

$$\xleftarrow{E_{Kpa}(m)}$$

$$D_{Ksa}(E_{Kpa}(m)) = m$$

Asymmetric encryption for **confidentiality**



Ks_A, Kp_A

Kp_A

Kp_A

$E_{Kpa}(m)$

$D_{Ksa}(E_{Kpa}(m)) = m$

Bob encrypts a message **m** with Alice's public key $\mathbf{Kp_A}$

➡ Nobody can decrypt **m**, except Alice with her private key $\mathbf{Ks_A}$

✓ Confidentiality without the need to exchange a secret key

RSA - Rivest, Shamir and Alderman

Key Size	1024 - 4096
Speed	~ factor of 10^6 cycles / operation
Mathematical Foundation	Prime number theory

Most widely used to secure network traffic

Adopted in 1977