Asymmetric keys

Ks_A, Kp_A

Kp_A

Kp_A

Alice generates a pair of asymmetric keys

- Ks_A is the secret key that Alice keeps for herself
- Kp_A is the public key that Alice gives to everyone (even Mallory)

➡ These two keys Ks_A and Kp_A work together

Asymmetric Keys - Functional Requirements

$D_{Ks}(E_{Kp}(m)) = m$ and $D_{Kp}(E_{Ks}(m)) = m$ for every pair $(\mathbf{Kp}, \mathbf{Ks})$

✓ Generating a pair $(\mathbf{Kp}, \mathbf{Ks})$ is easy to compute (polynomial)

✓ Encryption is easy to compute (either polynomial or linear)

✓ Decryption is easy to compute (either polynomial or linear)

◉ Finding a matching key $\mathbf{Ks}$ for a given $\mathbf{Kp}$ is hard (exponential)

◉ Decryption without knowing the corresponding key is hard (exponential)