Functional Requirements

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

- ✓ Generating a pair (Kp, 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 Ks for a given Kp is hard (exponential)
- ◉ Decryption without knowing the corresponding key is hard (exponential)

RSA - Rivest, Shamir and Alderman

Key Size	1024 - 4096
Speed	~ factor of 10^6 cycles / byte • Key generation: 10 - 100 ms • Encryption: 0.2 - 2 ms • Decryption: 5 - 10 ms
Mathematical Foundation	Prime number theory