RSA - encryption and decryption

Given $\mathbf{Kp = (e, n)}$ and $\mathbf{Ks = (d,n)}$

➡ Encryption : $\mathbf{E_{kp}(m) = m^e \bmod n = c}$

➡ Decryption : $\mathbf{D_{ks}(c) = c^d \bmod n = m}$

➡ **$\mathbf{(m^e)^d \bmod n = (m^d)^e \bmod n = m}$**

Other asymmetric cryptography schemes

Diffie-Hellman (precursor)

➡ No Authentication but good for key-exchange

El-Gamal

➡ Good properties for homomorphic encryption

Elliptic Curve Cryptography (widely used nowadays)

➡ Fast and small keys (190 bits equivalent to 1024 bits RSA)