RSA Encrypt/Decrypt Correctness Statement

\[ e \cdot d \equiv 1 \pmod{\phi(n)} \] // EEA using \( \lambda(n) \)

\[ e \cdot d \equiv 1 \cdot \phi(n) + 1, \] where \( t \) is an integer, \( x \in \mathbb{Z}_n^* \)

\[ x^{ed} \equiv x \pmod{n} \]

\[ x^{\phi(n)} \equiv 1 \pmod{n} \]

**Encrypt/Decrypt versus Signature**

**Encrypt/Decrypt**

- Objective: Anyone can encrypt message
- Only one person can decrypt
- \( \text{CSk} = (p, q, d), \text{PK} = (n, e) \)
- Decryptor: Everyone
- Encrypt: RSA Encrypt
- \( sk = (p, q, d) \)

**Signature**

- Objective: Only one person can compute a valid signature.
- Everyone can verify it
- \( \text{Signer} (p, q, d) \)
- \( \text{Everyone} (n, e) \)
- Compute \( (G, r) \)
- Broadcast Interest
- anybody can verify