RSA-2048

Key generation

1. Choose two 1024-bit prime numbers p and q.
2. Compute Let $n = pq$, choose $e \leftarrow \mathbb{Z}^*_{\phi(n)}$ and set $d \leftarrow e^{-1} \mod \phi(n)$.
3. Public key is (n, e) and secret key is (n, e, d).

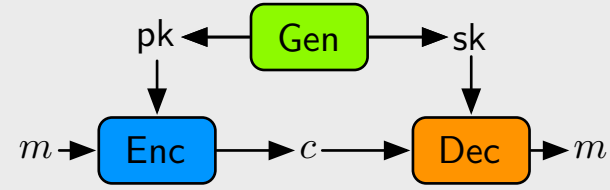
Encryption

1. Let $\mathsf{pad} : \{0,1\}^{128} \to \mathbb{Z}^*_n$ be a predefined embedding.
2. To encrypt $m \in \{0,1\}^{128}$, output $c \leftarrow \mathsf{pad}(m)^e \mod n$.

Decryption

1. To decrypt $c \in \mathbb{Z}_n$, compute $x \leftarrow c^d \mod n$.
2. Extract m form x and verify that $\mathsf{pad}(m) = x$.
3. Output $\perp$ in case of failure and m otherwise.

Public Key Cryptosystem



$$\forall(\mathsf{sk}, \mathsf{pk}) \leftarrow \mathsf{Gen} : \mathsf{Dec}_{\mathsf{sk}}(\mathsf{Enc}_{\mathsf{pk}}(m)) \equiv m$$