## 1.1 Description of the RSA Cipher

### Parameters

The three parameters

- $n$ = **module**,
- $e$ = **public exponent**,
- $d$ = **private exponent**,

are positive integers with

$$(1) \qquad m^{ed} \equiv m \pmod{n} \qquad \text{for all } m \in [0 \ldots n-1].$$

### Naive Description

The first idea is to set

$$M = C = \mathbb{Z}/n\mathbb{Z}, \quad K \subseteq [1 \ldots n-1] \times [1 \ldots n-1].$$

For $k = (e, d)$ we have

$$E_k : M \longrightarrow C, \qquad m \mapsto c = m^e \bmod n,$$

$$D_k : C \longrightarrow M, \qquad c \mapsto m = c^d \bmod n.$$

This description is naive for $n$ is variable, and (necessarily, as we'll see soon) a part of the public key. In particular the sets $M$ and $C$ vary.

### More Exact Description

We want to describe RSA in a form that fits the general definition of a cipher. To this end we note that for an $l$ bit number $n$ we have $2^{l-1} \leq n < 2^l$, thus fix the parameters:

- $l$ = bit length of the module (= "key length"),
- $l_1 < l$ bit length of plaintext blocks,
- $l_2 \geq l$ bit length of ciphertext blocks.

We construct a block cipher $M \longrightarrow C$ over the alphabet $\Sigma = \mathbb{F}_2$ with

$$M = \mathbb{F}_2^{l_1} \subseteq \mathbb{F}_2^{l_2} = C.$$

The key $k = (n, e, d) \in \mathbb{N}^3$ is chosen with ($2^{l-1} \leq n < 2^l$ or equivalently:)

$$\ell(n) := \lfloor \log_2 n \rfloor + 1 = l, \quad 1 \leq e \leq n-1, \quad 1 \leq d \leq n-1,$$

such that equation (1) holds. The symbol $\ell(n)$ denotes the number of bits, that is, the length of the binary representation of $n$.

To encrypt a plaintext block $m$ of length $l_1$ by $E_k$ we interpret it as the binary representation of an integer. The result $c$, a non-negative integer $< n$, has a binary representation by $l_2$ bits—completed with leading zeroes if necessary, or better yet, with random leading bits.

To decipher the ciphertext block $c$ we interpret it as a non-negative integer $c < n$ and transform it into $m = c^d \bmod n$.

### Really Exact Description

See PKCS = 'Public Key Cryptography Standard' #1:
`https://tools.ietf.org/html/rfc8017`.

### Questions to Address

- How to find suitable parameters $n, d, e$ such that (1) holds?
- How to efficiently implement the procedures for encryption and decryption?
- How to assess the security?

### Speed

Note that encryption and decryption are significantly slower than for common symmetric ciphers. (Estimates range up to a factor of roughly $10^4$.)