

RSA Cryptography

To generate the encryption and decryption keys, we can proceed as follows.

1. Generate randomly two “large” primes p and q .
2. Let $n = pq$ so that $\phi(n) = (p - 1)(q - 1)$.
3. Choose randomly a number e so that

$$\gcd(e, \phi(n)) = 1.$$

4. Find the *multiplicative inverse* of e modulo $\phi(n)$, i.e., find d so that

$$ed \equiv 1 \pmod{\phi(n)}.$$

This can be done efficiently using Euclid’s Extended Algorithm.

The encryption key is $K_E = (n, e)$ and the decryption key is $K_D = (n, d)$.

The encryption function is

$$E(M) = M^e \pmod{n}.$$

The decryption function is

$$D(M) = M^d \pmod{n}.$$

The whole process works since, if $0 \leq M < n$, we have

$$D(E(M)) = M.$$

This follows from the following Theorem.

Euler’s Theorem. *If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Let’s now prove that $D(E(M)) = M$.

Proof. Let $0 \leq M < n = pq$. Observe that if

$$C = E(M) = M^e \pmod{n} \iff C \equiv M^e \pmod{n},$$

then $C^d \equiv M^{ed} \pmod{n}$. Therefore

$$D(E(M)) \equiv M^{ed} \pmod{n}.$$

Since $ed \equiv 1 \pmod{\phi(n)}$, then

$$ed = 1 + k\phi(n), \quad k \in \mathbb{Z}.$$

Case (1). If $\gcd(M, n) = 1$, then Euler’s Theorem implies

$$\begin{aligned} M^{\phi(n)} &\equiv 1 \pmod{n} \implies M^{k\phi(n)} \equiv 1 \pmod{n} \\ &\implies M^{1+k\phi(n)} \equiv M \pmod{n} \\ &\implies M^{ed} \equiv M \pmod{n} \\ &\implies D(E(M)) = M. \end{aligned}$$

Case (2). If $\gcd(M, n) = p$ and $\gcd(M, q) = 1$, then $M = \beta p$ for $\beta \in \mathbb{N}$. Since $\gcd(M, q) = 1$, Euler’s Theorem implies

$$\begin{aligned} M^{\phi(q)} &\equiv 1 \pmod{q} \implies M^{q-1} \equiv 1 \pmod{q} \\ &\implies M^{k(p-1)(q-1)} \equiv 1 \pmod{q} \\ &\implies M^{k\phi(n)} \equiv 1 \pmod{q}. \end{aligned}$$

Therefore, $M^{k\phi(n)} = 1 + \alpha q$, $\alpha \in \mathbb{Z}$. Multiply both sides by $M = \beta p$ to get

$$M^{1+k\phi(n)} = M^{ed} = M + \alpha\beta pq = M + \alpha\beta n.$$

This last equality implies that $M^{ed} \equiv M \pmod{n}$, then $D(E(M)) = M$. ///