RSA Cryptography

Will Troiani

August 2020

Contents

1 Relevant number theory

First we define a function

Definition 1.0.1. Given a positive integer n, let d_n denote the number of integers m such that $\gcd(n, m) = 1$ where $m \leq n$. The function

$$\begin{aligned} \phi : \mathbb{Z}_{\geq 0} &\longrightarrow \mathbb{Z}_{\geq 0} \\ n &\longmapsto d_n \end{aligned}$$

is **Euler's Totient function**.

This function admits a surprising form:

Proposition 1.0.2. *Let $n \geq 0$ and write $n = p_1^{k_1} \cdot \ldots \cdot_n^{k_n}$. Then*

$$\phi(n) = p_1^{k_1-1}(p_1 - 1) \cdot \ldots \cdot p_n^{k_n-1}(p_n - 1) \tag{1}$$

Example 1.0.3. Applying (1) we find:

$$\phi(10) = \phi(2.5) = 2^{1-1}(2-1)5^{1-1}(5-1) = 1.1.1.4 = 4 \tag{2}$$

and indeed

$$\gcd(1, 10) = \gcd(3, 10) = \gcd(7, 10) = \gcd(9, 10) \tag{3}$$

RSA cryptography will hinge crucially on the following Theorem due to Euler:

Theorem 1.0.4 (Euler's Theorem)**.** *Let a be a number coprime to n. Then*

$$a^{\phi(n)} = 1 \pmod{n} \tag{4}$$

2 RSA Cryptography

A significant feature of RSA cryptography is that if A wants to send a message to B, then in fact only B needs to know the private key. That is, the private key can remain hidden *even from* A.

Say A is sending B a message m.

1. First, B picks two prime numbers, p, q say.
2. B makes the following calculations/choices:
   (a) Calculate $n = pq$,
   (b) Pick an integer e such that e is coprime to $\phi(n)$,
   (c) Calculate an integer d such that
   $$ed = 1 \mod \phi(n) \tag{5}$$
   (d) Then B sends A the integer e (these are the public key).
   (e) It is important that B keeps d to themselves (this is the private key).

Then, A write a message and encodes it in an integer in some way, for instance, by translating each letter into ASCII and then taking the integer which is given by the concatenation of these numbers, call this number m. Note, it is important that n is taken large enough so that $n > m$. Then A sends $c := m^e$ to B.

1. B receives c and performs the following calculation:
   $$\begin{aligned} c^d &= (m^e)^d & (6) \\ &= m^{ed} & (7) \end{aligned}$$
   Now, we have chosen d such that $ed = 1 \mod \phi(n)$, so there exists $k > 0$ such that
   $$ed = \phi(n)k + 1 \tag{8}$$
   Continuing with Calculation (7):
   $$\begin{aligned} m^{ed} &= m^{\phi(n)k+1} & (9) \\ &= (m^{\phi(n)})^k \cdot m & (10) \end{aligned}$$
   taking this equation modulo n, we now have (by Euler's Theorem (Theorem 1.0.4)):
   $$\begin{aligned} (m^{\phi(n)})^k \cdot m &= 1^k \cdot m \mod n & (11) \\ &= m \mod n & (12) \end{aligned}$$

and so B has uncovered the message.