RSA Correctness

Cohen Schulz

October 2024

1 Abstract

As an asymmetric encryption method, RSA utilizes both private and public keys to encrypt plain-text through the utilization of modular congruence. By exposing a public key, a series of steps can be done to encrypt any plain-text. This encrypted information can then be sent to the holder of the corresponding private key to "undo" the acts of encryption.

This process of "undoing" the encrypted plain-text, or decryption, can be proven through a correctness evaluation of $Dec(Enc(m)) = m$, where m is the plain-text message.

2 Introduction

2.1 Background

To begin, the environment in which we will be working in is defined as

$$\exists_{a,b,n} \in \mathbb{Z} \bullet a \equiv_n b \Leftrightarrow n \mid (a-b)$$

Or, simply

$$\exists_{a,b,n} \in \mathbb{Z} \bullet (a-b) \,\%\, n = 0$$

Now, by showing congruency within $mod(n)$ we can imply that for any n, $\exists_k \in \mathbb{Z} \bullet gcd(k,n) = 1$. Naturally, if $gcd(k,n) = 1$, then we know that k and n are co-prime. Now, we can assume that an inverse of k exists as follows

$$\exists_k^{-1} \in \mathbb{Z} \bullet k^{-1}k \equiv_n 1 \Rightarrow gcd(k,n) = 1$$

This is due to the fact that since $gcd(k, n) = 1$, a linear combination exists between k and n.

$$\exists_{s,t} \in \mathbb{Z} \bullet \quad 1 = sk + tn$$

This allows us to use the Extended Euclidian Algorithm to quickly find the inverse. However, this follows iff

$$a \equiv_n a'$$

Where a' can replace a in any congruence equation in $mod(n)$. By this existence, we can then utilize Fermat's Little Theorem

$$1\cdot 2\cdot 3\cdot \ldots (p-1) \equiv_p 1k\cdot 2k\cdot 3k\cdot \ldots (p-1)k$$

Where $\exists_{p,k} \in \mathbb{Z}$, so it follows that

$$1 \equiv_p k^{p-1}$$

And such exists an inverse, k^{-1}, where

$$k^{-1}\cdot k^{p-2} \equiv_p 1$$

Finally, we can utilize Euler's totient function, φ, where

$$\varphi(n) = |(n \in \mathbb{Z}) \in [0, n)|$$

Instinctively, the cases surrounding $\varphi(n)$ take three forms:

1. $\varphi(p) = p - 1$ iff p is prime
2. $\varphi(pq) = (p - 1)(q - 1)$ iff p is prime and q is prime
3. $\varphi(ab) = \varphi(a)\varphi(b)$ iff $gcd(a, b) = 1$

Or, simply as a product of its primes, p, as follows

$$\exists_n \in \mathbb{Z} \bullet n = p_1\cdot p_2\cdot \ldots \cdot p_i \Rightarrow \varphi(n) = n(1 - \frac{1}{p_1})\cdot (1 - \frac{1}{p_2})\cdot \ldots \cdot (1 - \frac{1}{p_i})$$

And thus, using both Fermat's Theorem and Euler's totient function, we can conclude for $\exists_n \in \mathbb{Z}$

1. $k^{\varphi(n)} \equiv_n 1$ iff $gcd(k, n) = 1$, for $\exists_k \in \mathbb{Z}$
2. $k^{p-1} \equiv_n 1$ iff $\exists_p \in \mathbb{Z} \bullet p$ is prime

2.2 RSA-Specific

Now that we have the background necessary to digest RSA, let's begin with defining our two most basic functions, $Enc(m)$ and $Dec(m)$, where m is the plain-text message. Where $Enc(m)$ represents encrypting m and $Dec(m)$ represents decrypting m.

$$Enc(m) = C \equiv_N m^e$$

$$Dec(m) = m \equiv_N C^d$$

Where $\exists_{p,q} \in \mathbb{Z} \bullet N = pq$, where p, q are distinct primes.
And $\exists_{e,d} \in \mathbb{Z} \bullet ed \equiv_{\varphi\ (N)} 1$, such that $m, c \in \mathbb{Z}_N$ and $e, d \in \mathbb{Z}_{\varphi(N)}$. And thus, we can define the public and private keys as

$$k_{pub} = (N, e)$$

$$k_{pr} = d$$

However, this is under the assumption that for any k, $\exists_{k^{-1}} \in \mathbb{N}$, shown by the following:

$$Assume\ \exists_{k,n} \in \mathbb{N} > 1 \bullet gcd(k, n) = 1$$

$$gcd(k, n)|n$$

$$gcd(k, n) = 1 \Rightarrow gcd(k, n) \mid 1 + st + kn\ for\ \exists_{s,t} \in \mathbb{Z}$$

$$1 = k^{-1}k + tn$$

$$k^{-1}k + tn \equiv_N 1 \Rightarrow k^{-1}k \equiv_n 1$$

$$\exists_k^{-1} \bullet kk^{-1} \equiv_n 1\ QED$$

Now that we have defined every element of RSA and its respective process of creation, we can now show that $Dec(Enc(m)) = m$.

3 Full Proof of Correctness

$$(m^e)^d \equiv_N m$$

$$ed \equiv_{\varphi\ (N)} 1 \ \Rightarrow ed = 1 + k\varphi(N)\ for\ \exists_k \in \mathbb{Z}$$

$$m^{ed} \equiv_N m^{1+k\varphi(N)} \equiv_N m \cdot m^{k\varphi(N)}$$

Case 1: Let $gcd(m, n) = 1$

$$m^{\varphi(N)} \equiv_N 1 \Rightarrow m^{k\varphi(N)} \equiv_N 1\ QED$$

Case 2.1: Let $gcd(m, n) \neq 1$ and Let $m = rq$ $(r < p)$

$$gcd(m, p) = 1 \Rightarrow m^{p-1} \equiv_p 1$$

$$m^{(p-1)(q-1)} \equiv_p 1 \Rightarrow m^{k\varphi(N)} \equiv_p 1^k$$

$$m^{k\varphi(N)} = 1 + pk'\ for\ \exists_{k\prime} \in \mathbb{Z}_N$$

$$m \cdot m^{\varphi(N)} \equiv_N m(1 + pk') \equiv_N m + mpk'$$

$$m \cdot m^{\varphi(N)} \equiv_N m + rpqk' \equiv_N m + rNk'$$

$$m \cdot m^{\varphi(N)} \equiv_N m\ QED$$

Case 2.2: Let $gcd(m, n) \neq 1$ and Let $m = sp$ $(s < p)$

$$gcd(m, q) = 1 \Rightarrow m^{q-1} \equiv_q 1$$

$$m^{(p-1)(q-1)} \equiv_q 1 \Rightarrow m^{k\varphi(N)} \equiv_q 1^k$$

$$m^{k\varphi(N)} = 1 + qk''\ for\ \exists_{k\prime\prime} \in \mathbb{Z}_N$$

$$m \cdot m^{\varphi(N)} \equiv_N m(1 + qk'') \equiv_N m + mqk''$$

$$m \cdot m^{\varphi(N)} \equiv_N m + spqk'' \equiv_N m + sNk''$$

$$m \cdot m^{\varphi(N)} \equiv_N m\ QED$$

Thus, we have proven that $Dec(Enc(m)) = m$.