RSA Cryptosystem

Brandyn Tucknott

Last Updated: 28 April 2025

Introduction

The RSA cryptosystem was named after its creators Rivest, Shamir, Adleman. It is the culmination of some wonderful results in number theory, most prominently Euler totient function. The motivation for the algorithm is this: there are three parties: a sender, receiver, and intercepter. The sender wants to send a message to the receiver without the intercepter knowing the contents of the message. The catch is, we assume the intercepter is always listening, and will always recieve the message. This is the setup for the development of a cryptographic algorithm, where the message can be encrypted, such that even when the intercepter sees the encrypted message, they cannot easily decrypt it. The reciever can then use the decryption key shared by the sender to revert the encrypted message back to its original form. The version of RSA introduced here is a simple version, and although mathematically sound, is still vulnerable to attacks. For example, the intercepter could send a message to alice, check the encrypted response, and work out the decryption scheme from there.

Prerequisites

A strong understanding of modular arithmetic and Euler's totient function is recommended to gain a working understanding of RSA. We will assume the reader has an understanding of modular arithmetic, and briefly cover Euler's totient function and Theorem results.

Euler Totient Function. Let $n \in \mathbb{N}$. Then the Euler totient function $\phi(n)$ counts the number of integers less than n which are coprime with n. For RSA, we need only know two things:

1. $\phi(p) = p - 1$ where p is prime.
2. $\phi(pq) = \phi(p)\phi(q)$ where p, q are prime.

Euler's Theorem. Let $a, n \in \mathbb{N}$ with $\gcd(a, n) = 1$. then

$$a^{\phi(n)} \equiv 1 \mod n$$

The Algorithm

Choosing the Components

1. Choose two large primes, p, q.
2. Compute $n = pq$.
3. Compute $\phi(n) = (p-1)(q-1)$.
4. Choose an encryption key e, where $2 < e < \phi(n)$.
5. Set d to be the multiplicative inverse of e mod $\phi(n)$, that is, $e \cdot d \equiv 1 \mod \phi(n)$.

The Algorithmic Process

Suppose Alice has a message m which she wants to send to Bob. RSA dictates that she should do the following: After generating all of the necessary components, put out the public encryption key (n, e). This is visible to anyone, including Bob and any malicious third parties. She should share with Bob her decryption key (n, d), and throw the rest of the info away.

1. Take the message m and raise it to the encryption key mod n. This will yield the encrypted message $c = m^e$.
2. She should then send this message to Bob, who is waiting to receive her message.
3. After receiving her message, Bob can take the encrypted message c and raise it to the decryption key mod n to restore it to the unencrypted message. That is, $c^d = (m^e)^d = m^{ed} \equiv 1 \mod n$.

Justification

Recall that by Euler's Theorem, $a^{\phi(n)} \equiv 1 \mod n$ if $a, n \in \mathbb{N}$ and a, n coprime. When we take a message m^{ed}, we rely on e, d being multiplicative inverses mod $\phi(n)$ so that $m^{ed} = m^{k\phi(n)+1} \equiv m \mod n$ for some $k \in \mathbb{N}$. Unless we guarantee it by design, note that m is not actually coprime with n, but with large enough p, q (i.e. hundreds of digits), the probability that they share a factor goes to 0.

Example

Let $m = 7, p = 5, q = 11$. Then we can compute

- $n = 5 \cdot 11 = 55$
- $\phi(n) = (5-1)(11-1) = 4 \cdot 10 = 40$
- Choose $e = 13$ (arbitraily; remember the only important restrictor is that $e, \phi(n)$ are coprime)
- Compute the multiplicative inverse of e, $d = 37$

Recognize that $\gcd(e, \phi(n)) = 1, \gcd(m, n) = 1$. Then the encrypted message that Alice sends to Bob is

$$c = m^e \mod n = 7^{13} \mod 55 \equiv 2 \mod 55.$$

Bob can decrypt this message by applying his decryption key d to the encrypted message c:

$$c^d \mod n = 2^{37} \mod 55 \equiv 7 \mod 55.$$

Observe that $c^d = 7 \mod 55$ is the same as our original message m, and thus we conclude that not only was Alice able to send an encrypted message to Bob, but also that Bob had the ability to decrypt it.

Sources

Shoup, V. (2009). A computational introduction to number theory and algebra (2nd ed.). Online version here