The RSA Algorithm

**Jack Griffiths, Max Johnson, James Lounds,
Harvey Olive, Oscar Oliver, James Taylor**

March 7, 2022

1   Introduction

RSA is an asymmetric cryptosystem first publicly proposed by Rivest, Shamir, and Adler in 1977 [2]. It has been used since at least 1973 in secret by intelligence organisations. An asymmetric cryptosystem is a way to encrypt a message with a "key" that is public - that is anyone can know its value without compromising the secuirty of the system - and a way to decrypt the encrypted message with a *private* key - if this key is known (with the public key), it is easy for an attacker to decrypt messages.
The security of the cryptosystem relies on the difficulty of factoring large prime numbers as we will see in section idk

1.1   Original Requirements

In their 1977 paper, Rivest, Shamir and Adler proposed the following criteria an asymmetric cryptosystem should satisfy
For an encyption procedure E, and decryption procedure D on a message M

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

2. D, E should be easy to compute

3. Revealing E does not reveal an efficient method for D

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

According to Diffie and Hellman's paper [1], satisfying (1)-(3) implies E is a "Trap-Door One-Way Function". With the added criterion of (4), E must be a "Trap-Door One-Way Permutation" - each output is a valid input to the function. A One-Way function is easy to compute one way, but hard to compute the inverse. A Trap-Door function has a hard to compute inverse, unless some private information is known, which makes the inverse easy to compute

1.2   Utility

Assymetric Encryption is fundamental to how modern networks communicate securely, albeit using a different algorithm Assymetry makes the ability to communicate securely with no private channel, and the ability to sign messages easy. There are symmetric algorithms for both, but assymetry removes some trust - since the other party cannot give access to your private key, but could give access to a shared key.

   The ability to send information about how to communicate securely over an insecure channel was vital in the development of secure email, and http protocols. Before modern encryption standards, parties would swap some physical data, be it a hard drive, or a post it note. From this shared data, which was known to be private, both parties could establish shared secrets generated by the original physical secret, using a publicly available algorithm. This reliance

on physical secrecy was not scalable for individuals to secure their communications. It would be akin to sending Google a letter with your password on. Diffie and Hellman [1] propose a system for creating a shared secret over an insecure channel using modular exponentiation.

The ability to sign a message is more unique to assymetric cryptography. If we had a symmetric system, in order for Bob to prove to Charlie that Alice sent him a message, Bob must reveal Alice and Bob's shared secret to Charlie. Since Charlie now knows the secret, she can decrypt any message Alice and Bob sent to one another with this key However, in a public key system, anyone can know Alice's public key, so for Bob to prove to Charlie that Alice sent him a message, he only needs to tell Charlie Alice's public key, maintaining the privacy of Alice's key pair. In their paper [2], Rivest, Shamir and Adler propose a signing system in which the Alice decrypts her plaintext message, and sends it to Bob (with the message). Since $E(D(M)) = M$, Bob can encrypt the signature with Alice's public key, and check that the messages match. This can be optimised by hashing (a one way map) the message before decrypting it. That is $S = D(\mathcal{H}(M))$ Since hashes are a fixed length we can require the hash to be smaller than the size of a message block, and only need to transmit one more block instead of twice as many. This signature algorithm is very rarely used, in favour of DSA, or ECDSA [citation needed].

1.2.1 Blockchain

At its core, a blockchain is a long text file that lots of people have access to (a distributed ledger). But how can one ensure that Alice did in fact send Bob something. Alice can sign her transaction with her public key. Her public key is typically her address, or identifier within the network, so we know the person who has the private key to the "account" something was initially sent to has signed the transaction.

However, more utility can be gained using mutli-sig. All n members of a group who want to exchange some thing broadcast this to the blockchain. To do this, any one member of the group can submit n public keys to the network, not necessarily including their own. On creation, the creator tells the network how many group members need to agree to move funds.

1.2.2 PGP

PGP - Pretty Good Privacy - is an open source set of standards to encrypt and decrpyt messages, and create a "web of trust".

To encrypt, first the encrypter generates a random (symmetric) encryption key. The message is encrypted with this key, and the key is encrypted with each of the recievers' private keys. Each of these reciever-specific encrypted keys is prefixed with the reciever's fingerprint - a shorter representation of their private key.

To decrypt, the reciever locates their fingerprint, and decrypts the corresponding message. They then use the message in this key to decrypt the main

message.

PGP also offers signatures, which can be done with either RSA or DSA. Since any message can be signed, other people's public keys can be signed. PGP creates a "web of trust" by allowing users to publish a signed public key. If a large number of people you trust (read people whose private key you have) sign a public key, you can be reasonably convinced the public key is legitimate.

1.2.3 TLS

TLS - Transport Layer Security - is responsible for securing HTTP communications. TLS relies on no single encryption or signature standard, instead agreeing a "cipher suite" as its first step. To convince your browser you're speaking to the right server, the server sends a signed message (certificate) including information about who they are, and a message "vouching" for the certificate's legitimiacy. These "vouches" are signatures by Certificate Authorities: entities that are trusted to sign certificates.

Now the client knows the server is who they say they are, they can either choose a random number, encrypt it with the server's public key and send it. This is now the symmetric key. Or, they can perform Diffie-Hellman Key Exchange [1]. The second methodi is preferred since should the server's private key be compromised, no communications can be decrypred.

2 The Proposed Cryptosystem

2.1 Definitions

$$E(M) \equiv M^e \ (mod \ n), \quad D(M) \equiv M^d \ (mod \ n)$$

with $n := p \cdot q$ and p, q are prime, and $e^{-1} \equiv d \ (mod \ \phi(n))$.

In order to generate a private and public key, we first need to find 2 large primes p, q. It is important they remain secret as if an attacker were able to factorise $n := p \cdot q$, they would easily be able to compute the decryption key. We can then choose a random d such that $GCD(d, \phi(n)) = 1$, that is d has an inverse $(mod \ \phi(n))$. Since p, q are prime, $\phi(n) = (p-1) \cdot (q-1)$. We can then compute $e \equiv d^{-1} \ (mod \ \phi(n))$, and publicly send (e, n) without revealing d.

2.2 Proof

Theorem 1. *If p, q are prime, then $\phi(p \cdot q) = (p-1) \cdot (q-1)$*

Proof. Since p, q are prime, pq only has factors $\{1, p, q, p \cdot q\}$, so for any d which is not coprime to $p \cdot q$

$$\text{Let } k := gcd(d, p \cdot q) \text{ , } k \neq 1 \text{ since } d \text{ is not coprime to } p \cdot q$$
$$d = k \cdot 1, \text{ or } d = k \cdot p, \text{ or } d = k \cdot q$$

In the first case, for d to divide $p \cdot q$, k must be p or q since p, q are prime. Both of these are covered in the $d = k \cdot p$ or $d = k \cdot q$ cases.

Let's define $\phi'(n)$ to be the cototient of n,

$$\phi'(n) := n - \phi(n)$$

$\phi'(n)$ is the number of naturals *less than* or equal to n which are *not* coprime to n. That is, $\phi'(n)$ is the number of values of k such that $0 < d \leq p \cdot q$.

$$0 < k \cdot p \leq p \cdot q \Rightarrow k \in \{2, 3, \ldots, q\}, d \in \{2p, 3p, \ldots, (q-1) \cdot p, \ q \cdot p\}$$
$$0 < k \cdot q \leq p \cdot q \Rightarrow k \in \{2, 3, \ldots, p\}, d \in \{2q, 3q, \ldots, (p-1) \cdot q, \ p \cdot q\}$$
$$0 < k \cdot 1 \leq p \cdot q \Rightarrow k \in \{p, \ q, \ p \cdot q\}, d \in \{p, \ q, \ p \cdot q\}$$

So $\phi'(n)$ is the cardinality of the union of these sets

$$\phi'(p \cdot q) = |\{p, \ q, \ p \cdot q\} \cup \{2p, 3p, \ldots, (q-1) \cdot p, q \cdot p\} \cup \{2, 3, \ldots, (p-1) \cdot q, p \cdot q\}|$$
$$= |p, 2p, 3p, \ldots, (q-1) \cdot p, \ q, 2q, 3q, \ldots, (p-1) \cdot q, \ p \cdot q|$$
$$= (q-1) + (p-1) + 1$$
$$= p + q - 1$$
$$\Rightarrow \phi(p \cdot q) = p \cdot q - \phi'(n)$$
$$= p \cdot q - (p+q-1) = p \cdot q - p - q + 1$$
$$= (p-1) \cdot (q-1)$$

$\square$

Theorem 2. *Fermat's Little Theorem*

Proof. To be done $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

Theorem 3. *If p, q are prime and $n := p \cdot q$, then for any $d \equiv e^{-1} \ (mod \ \phi(n))$*

$$E(M) \equiv M^e \ (mod \ n), \quad D(M) \equiv M^d \ (mod \ n)$$

$$\Downarrow$$

$$D(E(M)) \equiv M \ (mod \ n) \equiv E(D(M)) \ (mod \ n)$$

Proof. If a prime p does not divide M,

$$
\begin{aligned}
M^{\phi(p)} &\equiv M^{p-1} \ (mod \ p) \equiv 1 \ (mod \ p) && (by \ Fermat's \ Little \ Theorem) \\
&\equiv M^{k\phi(n)} \ (mod \ p) \equiv 1 \ (mod \ p) && (Since \ \phi(p) \ divides \ \phi(n)) \\
M^p &\equiv M^{k\phi(n)+1} \ (mod \ p) \equiv M \ (mod \ p) && (By \ multiplying \ by \ M)
\end{aligned}
$$

The same can be argued for q

By the Chinese Remainder Theroem:

$$
\left.
\begin{aligned}
M^{k\phi(n)+1} &\equiv M \ (mod \ p) \\
M^{k\phi(n)+1} &\equiv M \ (mod \ q)
\end{aligned}
\right\}
\Rightarrow M^{k\phi(n)+1} \equiv M \ (mod \ n)
$$

By definition, $e \equiv d^{-1} \ (mod \ n)$, so

$$
\begin{aligned}
e \cdot d &\equiv 1 \ (mod \ \phi(n)) \\
e \cdot d &= k\phi(n) + 1 && (for \ some \ k \in \mathbb{N}) \\
\Rightarrow D(E(M)) &\equiv M^{e \cdot d} \ (mod \ n) \\
&\equiv M^{k \cdot \phi(n)+1} \ (mod \ n) \\
&\equiv M \ (mod \ n)
\end{aligned}
$$

$$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$$

2.3   Efficient Computation

2.3.1   Modular Exponentiation

Consider the binary representation of some exponent e:

$$e = 2^0 \cdot e_0 + 2^1 \cdot e_1 + \ldots + 2^n \cdot e_n$$

By the rules of indicies,

$$M^e = M^{2^0 \cdot e_0 + 2^1 \cdot e_1 + \ldots + 2^n \cdot e_n}$$
$$= M^{2^0 \cdot e_0} \cdot M^{2^1 \cdot e_1} \cdots M^{2^n \cdot e_n}$$

So in a ring $\mathbb{Z}/n\mathbb{Z}$,

$$M^e \equiv M^{2^0 \cdot e_0} \cdot M^{2^1 \cdot e_1} \cdots M^{2^n \cdot e_n} \ (mod \ n)$$
$$\equiv (M^{2^0 \cdot e_0} \ (mod \ n)) \cdot (M^{2^1 \cdot e_1} \ (mod \ n)) \cdots (M^{2^n \cdot e_n} \ (mod \ n)) \ (mod \ n)$$

We can easily generate the elements $M^{2^i e_i}$ by repeatedly squaring M. We only include this element if e_i is 1, that is the bit is true. So we only need to square M $log_2(e)$ times, then perform at most $log_2(e)$ multiplications and remainder calculations. But space is where the main savings are: the largest number we need to store will necessarily be less than n. We only need to store the running total, and the current square (e is given to us). So we only need to store 2 n-sized blocks.

2.3.2   Prime Generation

There are a variety of prime generation algorithms, but we will only consider the probabilistic method in RSA's paper. If a is prime less than a, then:

$$gcd(a, b) = 1, \ and \ J(a, b) \equiv a^{(b-1)/2} (mod \, b)$$

Where J is the Jacobi symbol. However, this is also true with probability $\frac{1}{2}$ when b is not prime. So if we test r values of a, and the equations are valid for each a we choose, there is only a $(\frac{1}{2})^{100} \approx \frac{1}{1.26 \cdot 10^{30}}$ chance b is not prime. Other algorithms exist, and in our implementation, we used python's `Crypto.Util.number.getPrime`, which generates a random number and checks it with a probabilistic sieve.

References

[1] W. Diffie and M. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[2] R.L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.