The RSA Algorithm

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

March 4, 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 tp 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 tp 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

2 The Proposed Cryptosystem

2.1 Definitions

Preamble

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

with $n \coloneqq p \cdot q$ 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 $n \coloneqq p \cdot q$, 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

2.2.1 Lemma 1

Statement: if p, q are prime, then $\phi(n) = (p-1) \cdot (q-1)$

Proof:
If p is prime, then $\phi(p) = p - 1$, since $\phi(p)$ is the number of naturals less than p which are coprime to p. Only 1 is a factor of p that is less than p, so $\phi(p) = p-1$

Consider a 2D grid of the numbers 1 to mn with m columns and m rows.

$$\begin{array}{cccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ m & 2m & 3m & \cdots & nm \end{array}$$

Consider the rth row

$$r \quad m+r \quad 2m+r \quad \cdots \quad (n-1)m+r$$

If d is the greatest common divisor of r and m, then if $d > 1$ no number in the rth row of the table is relatively prime to mn, since d divides $(km + r)\, \forall k$. So the rows containing numbers which are coprime to mn have $gcd(r, m) = 1$. By the Euclidean algorithm, $gcd(km + r, m) = 1 \Leftrightarrow gcd(r, m) = 1$, meaning each entry in the rth row is relatively prime to m. Exactly $\phi(n)$ of these will be coprime to n, and thus mn. So there are $\phi(m)$ rows, each containing $\phi(n)$ entries coprime to mn.
Therefore $\phi(mn) = \phi(n) \cdot \phi(m)$. And if $\phi(p) = p - 1$, $\phi(q) = q - 1$
$\phi(pq) = (p-1) \cdot (q-1)$

2.2.2 Lemma 2

Statement: Fermat's Little Theorem
Proof:
Later

Statement: If p, q and $n \coloneqq p \cdot q$, 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, $M^{\phi(p)} \equiv M^{p-1} \, (mod \, p) \equiv 1 \, (mod \, p)$ by Fermat's Little Theorem
Since $\phi(p)$ divides $\phi(n)$, $M^{\phi(p)} \equiv M^{k\phi(n)} \, (mod \, p) \equiv 1 \, (mod \, p)$ By multiplying by M, $M^p \equiv M \, (mod \, p)$.
By the Chinese Remainder Theroem:
$M^{k\phi(p)+1} \equiv M \, (mod \, p), \; M^{k\phi(q)+1} \equiv M \, (mod \, q) \Rightarrow M^{k\phi(n)} \equiv M \, (mod \, n)$
Therefore if $e \cdot d = k\phi(n) + 1$, that is $e \cdot d \equiv 1 \, (mod \, \phi(n))$, or $e \equiv d^{-1} \, (mod \, \phi(n))$ then $D(E(M)) = (M^e)^d = M^{e \cdot d} \equiv M \, (mod \, n)$

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.