The RSA Encyption Algorithm

Tom Nicholls

November 20, 2012

Published in 1978, the Rivest-Shamir-Aldeman (RSA) scheme [1] is one of the most widely accepted and implemented approaches to public-key encryption. The RSA algorithm is based upon the difficulty of factoring large integers. It acts as a block cipher in which for some n, the ciphertext and plaintext are integers between 0 and n. Typically, n is less than 1024 bits or 309 decimal digits. Hence, n is less than 2^{1024}.

The operation of the RSA encryption scheme has three parts: Key generation, Encryption and Decryption. The description of this scheme uses the common placeholder names of Alice and Bob inkeeping with tradition set out by Bruce Schneier [2].

1 Key Generation

RSA is an example of an asymmetric key algorithm, in which a **public** key and a **private** key are utilised. The public key is shared and known with everyone and used in the encryption process. The messages encrypted with the public key can only be decrypted using the matching private key. The following process is used to generate the required keys:

1. Choose two distinct prime numbers p and q.
    - These are chosen at random and kept private.
2. Calculate $n = pq$.
3. Calculate $\phi(n) = (p-1)(q-1)$, where $\phi(n)$ is the number integers k such that $1 \leq k \leq n$ and $gcd(n,k) = 1$.
4. Choose e such that $1 < e < \phi(n)$ and e and ϕ are coprime
5. Determine d as $d = e^{-1} \, (mod \, \phi(n))$. Here d is the multiplicative inverse of $e \, mod \, \phi(n)$.
    - This is the same as solving for d give $(de) = 1 \, mod \, \phi(n)$.

Therefore the private key consists of [d,n] and the public key consists of [e,n]. The private key must be kepy secret whereas the public key can be shared. p, q and ϕ must also be kept secret as they were used to calculate d.

2 Encryption

Bob wants to send a message **M** to Alice. Alice sends Bob her public key $K_a = e, n$ and keeps her private key secret. Bob turns **M** into an integer m, such that $0 \leq m < n$ using a previously agreed method. the then computes the ciphertext c corresponding to

$$c = m^e \, (mod \, n)$$

Bob then sends c to Alice.

3 Decryption

Alice receives ciphertext c from Bob. She can recover the message m from c using her private key d by computing

$$m = c^d \, (mod \, n)$$

Given m she can find the original message **M** by reversing the agreed method.

4 Explanation

As can be seen above, encryption and decryption are of the form

$$c = m^e \, mod(n)$$

$$m = c^d \, mod(n) = (m^e)^d \, modn = m^{ed} \, mod(n)$$

For this algorithm to be securely used for public-key encryption, the following requirements must be satisfied.

1. e, d and m can be found such that $m^{ed} \, mod(n) = m$ for all $m < n$.
2. $m^e \, mod(n)$ and $c^d \, mod(n)$ are relatively easy to compute, for all values of $m < n$.
3. It is infeasible to determine d given e and n.

Using the Euler totient function $\phi(n)$ as described above it can be seen that

$$ed\, mod(\phi(n)) = 1$$

$$ed = 1\, mod(\phi(n))$$

$$d = e^{-1}\, mod(\phi(n))$$

which satisfies the first condition.

The description of this encryption scheme is based upon the description given by William Stallings [3]

References

[1] A. Rivest, R.; Shamir and L. Adleman, Communications of the ACM (1978).

[2] B. Schneier, *Applied Cryptography: Protocols, algorithms and source code in C*, Second ed. (Wiley, 1996).

[3] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Fifth ed. (Pearson, 2011).