Review “RSA”

Name: Wenhui Zhang
Email: wuz49@ist.psu.edu

Paper Name :

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

Contribution:

This paper proposed an encryption method named after authors’ names, RSA. This method is based on the idea that factorization of integers into their prime factors is hard.This method strengthens protection of decryption key even when encryption key is publicly revealed. This paper tells us details on “public-key cryptosystem”, which is the first implementation for theoretical methods proposed by Diffie and Hellman.

Motivation:

We lack efficient, high-quality encryption techniques for this emerging “electronic mail” era. Other encryption methods has issues with “key distribution problem”, which is the most important component in secure transmission.

Related works:

There are two parts of previous related works: (1) key distribution refers to ways of securing communications without having to trust KDC, e.g. Diffie and Hellman proposed the idea of public key cryptosystem; (2) digital signatures refers to ways of verifying a message from claimed senders in a “message dependent” and “signer-dependent” manner.

Methodology:

RSA is acquires security due to cost of factoring large numbers is large. The algorithm is based on exponentiation in a finite field over integers modulo a prime, as shown below:

$a^{ø(n)}$mod N = 1 , where gcd(a,N)=1

Then in RSA, we have:

$N=p.q$

$ø(N)=(p-1)(q-1)$, we could carefully chosen e & d to be inverses mod $ø(N)$

$e.d=1+k.ø(N)$ for some k

hence :

$C^d = (M^e)^d = M^{1+k.ø(N)} = M^1.(M^{ø(N)})^q = M^1.(1)^q = M^1 = M$ mod N

Results:

The security of RSA encryption method is proved using cryptanalytic approach: (1) factoring n does not work effeciently when n is big; (2) mathematical attacks is hard to achieve as its difficulty of computing ø(N), by factoring modulus N is high; (3) computing ø(N) or determining d without factoring is hard; (4) computing D is as difficult as factoring.

Take away:

The key to break RSA is finding a way of efficiently factoring large numbers. The world need mathematicians for theories behind this. As far as mathematicians who could work it out is not born yet, RSA is pretty secure to use.