Some understanding about RSA ep system

Based on the Euler theorem, RSA use some mathematical transformation to ep some data message. It can also be used for digital signature and identity authentication. This algorithm is presented by three young professor from MIT in 1977, and named by their last name, Rivest, Shamir and Adlernan. A fact in number theory field is that though compute the product of two large number is simple, it is extremely hard to factor it back into the primes. Compare with *Diffie-hellman* algorithm, RSA have the obvious superiority because the pair don’t have to involve in the ep process at the same time. Others, it is suit for electronic mail system.

Before 1976, all the ep algorithm is in a same mode, 1),A choose a mode of ep regulation

2)B choose the same regulation to DP it. Because of the same rule, we call this way to *symmetric-key algorithm.* The biggest weakness of this way is that A must tell B the ep rule to B, otherwise, he can’t DP it. But after 1976, *Diffie-hellman* algorithm had been invented, and based on that, RSA appeared. Now, the longest security key which had been cracked length is 768, that means a security key which have a length more than 1024 is almost safe to most average person, if you use a key which have 2048 digit, it is too safe to us.

The principle of this algorithm is based on a little number theory.

1. co-prime relationship

If a pair of positive integer have no common factor except 1, we call this pair of number is co-prime, for example, 13 and 61.

1. Euler function

Given any positive integer n, how many positive integer smaller than n can constitute a relatively prime relationship? The way to calculate this value is Euler function. the calculate method is not difficult, but in order to get the final formula, we must discuss the situation,

1. n=1

f(n)=1.

1. n is a prime number

f(n)=n-1.

1. If n=p^k (p is a prime number, k>1 and is a integer)

f(p^k)=p^k-p^(k-1)

this formula can also written in another form   
 f(p^k)=p^k-p^(k-1)=p^k(1-1/p)

1. If n can decomposed into two mutually integer integers

n=p1\*p2

then f(n)=f(p1p2)=f(p1)f(p2)

for example f(56)=f(8)f(7)=24.

1. By the fact that any positive integer greater than 1 can be written as a series of prime numbers, according to the corollary of article 4,

f(n)=f(Pk1)f(Pk2)……f(Pkr)

and according to the corollary of article 3

f(n)=n(1-1/P1)(1-1/P2)…(1-1/Pr).

This is the calculation process, if we want to calculate 1323’s Euler function.

f(1323)=f(3^3\*7^2)=1323(1-1/3)(1-1/7)=756

The reason we use the Euler formula is that it can greatly simplify some operations, for example 7 and 10 are qualities, according to Euler theorem, 7^(f(10))=1(mod 10), we know that f(10)=4, so we can immediately know 7^4k=1(mode 10)

The latest concept is Modular multiplicative inverse

. If the two positive integer a and n are prime, we must find a integer b which can let ab-1 divisible by n. then we call b as modal elements to a. it is worth mentioning that modal element are not unique.

That is all the mathematical tools we would use in this paper. Then we would look at the generate steps of key. If Tony and Friday want to perform encrypted communication, how could he generate a public key

1. Select two prime numbers p and q randomly

In our example, he choose 61 and 53. But we must know that the bigger these prime number is, more difficult to crack to other one.

1. Calculate the product of this pair of number n, the result is 3233.

The length of n is the length of key 3233 written in binary is 110010100001, the length of this number is 12, so the length of the key is 12, in practical application, the length is always 1024, even 2048 in important occasion.

1. Calculate f(n)

By the formula

f(n)=(p-1)(q-1)

f(3233)=60\*52=3120.

1. Choose a integer e randomly, it must between 1 and f\*n) and e must quality with f(n). in this example, we choose 17.
2. Calculate the Modular multiplicative inverse e for f(n).

The so called Modular multiplicative inverse is a integer d which let ed be divided by f(n) by 1. This is the solution of the following formula .

ex=f(n)y=1

e=17,f(n)=3120,so a set of the solution of this equation is (x,y)=(2753,-15). d=2753.

1. Package n and e to a public key, package n and d to a private key

In the example ,the public key is (3233,17)，the private key is (3233,2753).

From this example we can see the whole process of RSA algorithm. In this turn, six number had been appeared. P, Q, N, f(n),e and d. in this six numbers, public key use n and e, and all the other 4 numbers are not openly. The most important is d because d and n make a private key. If d leaked, equivalent to private key leaked.

But, is there a possibility that deduce d only by n and e? From the process, we can easily know that if n can be factorized, that mean the private key can be cracked. However, it is very hard to factory a large integer. Now, only violent crack can we do to calculate it. We can factory 3233 to 61\*53, but if you want to factory the following number

1230186684530117755130494958384962720772853569595334792197322452151726400507263657518745202199786469389956474942774063845925192557326303453731548268507917026122142913461670429214311602221240479274737794080665351419597459856902143413

it is the product of

33478071698956898786044169848212690817704794983713768568912431388982883793878002287614711652531743087737814467999489  
 ×  
3674604366679959042824463379962795263227915816434308764267603228381573966511279233373417143396810270092798736308917

This is the open limit. If we use larger number, it is almost completely safe.

However, by the rapid development of quantum computer, there is a new way to crack RSA algorithm. In *science July 2015,* a paper written by 9 authors. In their paper. Shor’s algorithm for factoring integers is one of the examples where a quantum computer outperforms the most efficient known classical algorithms. And they find an implementation method. According to their paper, they can decomposed 15 into 2 prime numbers based on 2 quantum. Account the pace of development, maybe in 20 years, rsa is no longer a safe algorithm. We must know that technology development is faster than our image. We also know that it is the era of data now.

Though this algorithm had been reported that by the noise, it has been cracked in a length of 4096, the problem is to implement rather than method. It was so widely used that despite the attack is endless was still not broken. It is almost certain that there is new technology in our lifetime, but this algorithm will use widely at least 20 years.