A realization about RSA ep system

Based on the Eular 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. Eular 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 Eular 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.