Analysis of Random Function and its Application in the Encryption Algorithm

She Wei[1,a] , Xie Huijuan[2,b]

[1] Hainan Institute of Science and Technology, 571126, Haikou, China

[2]Hainan College of Economics and Business, 571127, Haikou, China

[a]694394619@qq.com, [b]360088369@qq.com

Keywords: Random Number, Shamir Encryption, RSA Encryption, Seeds

Abstract. One of the important characteristics of the random number is unpredictable, and the rear number will be generated without any relationship with the generated random number, the real random number is generated physically, but relatively high technology is needed, in fact pseudo-random numbers that has similar statistical characteristics of random numbers are enough to use, it has a random numbers have been applied in the Shamir encryption algorithm and RSA encryption algorithm.

Introduction

The random number is generally divided into pseudo-random numbers and true random numbers, the pseudo-random numbers generally used for simulation, testing and financial fields are generated easily, and used more conveniently, the true random numbers used in the more safer field are not crack easily.

C language commonly used function rand() to generate a random number, in fact it’s no at really but pseudo-random number. When it is called repeatedly, we can get a set of random numbers with the same sequence, which is a coefficient take the seed as a benchmark and recursive formula, when this coefficient is very large and normally distributed, a pseudo-random number will be generated. Because the seeds remain unchanged, the random number is unchanged when the computer shuts down. Therefore, in order to get a true random number in the program, usually different random seeds should be given.

Random Number Generation

The Application of Function Rand().

The format function rand() is “int rand (void)”;.The head file of stdlib.h should be added when the function of rand() is being used. The following example is that five integers between 0-9 are generated randomly.

```
#include"stdio.h"
#include"stdlib.h"
. . . …
CreateRand1()
{ int k;
  for(k=0;k<=4;++k)
  {    printf("%d\t",rand()%10); }}
```

The results of two running the program indicate that function rand() can only obtain a set of pseudo-random random numbers with the same sequence.

The Application of the Function of Strand ().

The C language provides a random number generator (the function of stand()) that can change the value of seed, the following example generates 5 random integers which range is between 0 and 9.

The algorithm of inputting the same or different seeds by keyboard is as follows:

```
#include"stdio.h"
#include"stdlib.h"
… …
CreateRand2()
{
  int k;
  unsigned seeds;
  printf("Please input the seeds: ");
  scanf("%u",&seeds);
  void strand(seeds);
  for(k=0;k<=4;++k)
  {
    printf("%d\t",rand()%10);
  }
}
```

A set of random numbers with the same sequence can be obtained by inputting the two same seeds, or a set of different random numbers can be obtained by inputting the two different seeds.

The algorithm of taking the function of time()as a random seed is as follows:

```
#include"stdio.h"
#include"stdlib.h"
#include"time.h"
… …
CreateRand3()
{
int k;
  long *p1;
  void strand(time(p1));
  for(k=0;k<=4;++k)
  {
    printf("%d\t",rand()%10);
  }
}
```

The function in seconds save the current system time and the interval of Greenwich Mean Time into the location referred by timer that is not a null pointer [1]. When the function of time() is used, the head file(time.h)must be added.

The two results shows that two sets different random numbers can be obtained by two different seeds by taking the function of time() as seeds.

A random number which value is between 0 and RAND_MAX that equals 32767 will be returned by calling the function of rand() in the C language function library [2]. The sentence (m=rand()%(b-a+1)+a;) can generate random number that is between a and b.

The Application of Random Number in Cryptography.

Due to the unpredictability of the random number, can act as a key role in the cipher text and the true random numbers can't be repeated, even if the attacker obtained the key information for a time, but it is difficult to infer next secret information, of course plaintext can't be gotten. Therefore, true random number had been applied widely in the information security [3]. Fig 1 show the process of encryption and decryption in the communication system, where the random numbers are generally used in the plaintext encryption.

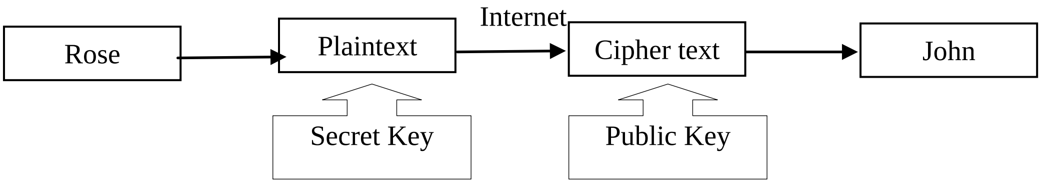

Fig1 Encryption and Decryption in the Communication System

In cryptography, the random number is often used in the plaintext encryption in order to ensure the security of the information. The following is that the random numbers were used in the Shamir encryption algorithm and RSA encryption algorithm.

The application of Random numbers in Shamir secret sharing scheme.

Shamir secret sharing scheme divide a key into n shared secret keys, and assigned secretly to n different users, more than k users can effectively restore the key, less than k users can't retrieve the key, so effectively eliminates the losses because of excessive concentration of a master key or the plots of a few objects. Shamir secret sharing scheme was used in the key in computer network management; the random numbers were often applied to the generating polynomial coefficients and selecting n elements of Shamir secret sharing scheme.

The application of Random numbers in RSA.

RSA encryption algorithm is a non-symmetric encryption algorithm; it not only can be used in information encryption but also be used for digital signature. It is especially suitable for the computer network environment, can output the encryption key in manner of phone books for a large number of users on the network, if a user wants to securely communicate with other users, only needs to find out each other's encryption key from the public key directory, that can be used to encrypt the transferring information, when the partner receives the information, decrypts the key with it and reads the information. The random numbers can be used to create two distinct large prime numbers and the encryption key is generated randomly, the application is shown in Fig2.

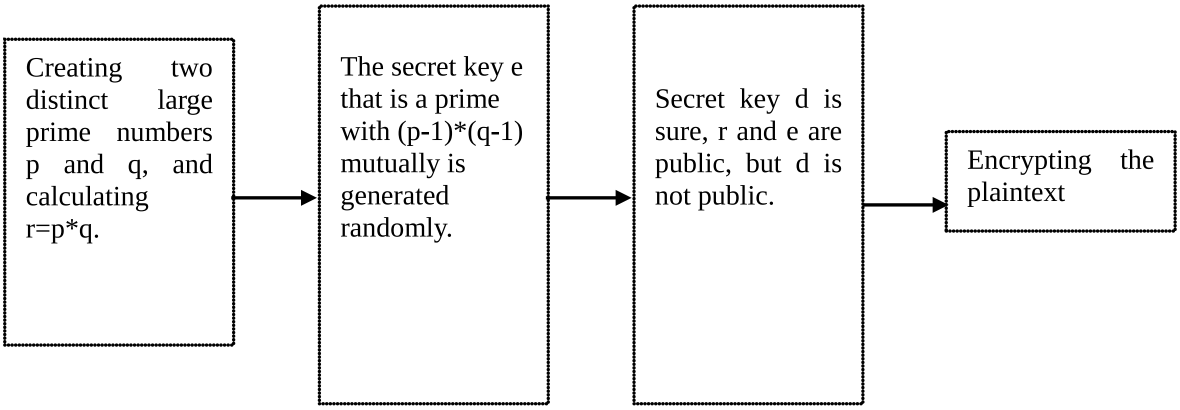
Creating two distinct large prime numbers p and q, and calculating r=p*q.
The secret key e that is a prime with (p-1)*(q-1) mutually is generated randomly.
Secret key d is sure, r and e are public, but d is not public.
Encrypting the plaintext

Fig2 The Process of the Application of Random Numbers in RSA

Summary

The function of rand() can generate random numbers, only ensures that the first random is random and memories the result. The function of strand() can change the value of seed and get seed from the function of time(), can get different random numbers. Dierent random number generators have been proposed using dierent architectures and algorithms and prototyped in FPGAs[5].The random numbers are widely used in many fields related to the encryption algorithm, and widely used in mathematical modeling, electronic commerce, network security, industrial control, the gambling industry and cryptography and so on [3].

References

[1] Zheng.J.H.C Language Programming Fundamentals [M].Wuhan University Publishers, 2011:236-238.

[2] Sun.H.Q. FAQ and Examples of Algorithm in C Language [M]. Heilongjiang Education Press, 2011:83-84.

[3] Wang.H.J. The Online Test and Subsequent Processing of Random Number[J]. Taiyuan University of Technology, 2012:05-20.

[4] Li.W.C. The Computer Information Security Technology[M]. National University of Defense Technology Press, 2010:40-52.

[5] Viktor Fischer and Milos Drutarovsky, True random number generator embedded in recongurable hardware, Proc. of CHES 2002 (2003), 415-430.