An Efficient Method of Generating Random Numbers from Congruence Equations for Cryptographic Applications

Richa Agarwal[1], Gaurav Agarwal[2]

[1]*Research Scholar, Computer Science and Engineering Department,*
Invertis University,Bareilly

[2]*Assistant Professor, Computer Science and Engineering Department,*
Invertis University,Bareilly

Abstract - As in today's scenario, security is the major issue for everyone, so for that situation random numbers plays a vital role for security purposes. Random numbers are those numbers that occurs in a sequence such that it becomes impossible to predict future values based on past or present one and such numbers are also required to be independent. These can be used for different purposes in cryptography for security purposes or for secure communication. In this paper, pseudo-random numbers are generated using Congruence equations.

Keywords- congruence equations, Chinese remainder theorem, randomness, pseudorandom generator, key generation, private-key encryption.

I. Introduction

In cryptography, there are various uses of random numbers, like in encryption keys, also helps in creating initial parameter values, and also to introduce random nonces. Generally, random numbers originate from Pseudorandom Number Generator(PRNG) [1]. A pseudorandom generator takes input or also known as seed value, from user and generates random numbers as output. In pseudorandom generator, no one can predict pattern which can be termed as *randomness*. Congruence equations are the equations of given form: f(x)≡b (mod m), where the values should be 0≤x<m. Such an equation may have one or more solutions. There are different techniques to generate pseudorandom numbers such as Blum blum shub, middle square method, linear congruential generator, etc.

A random number generator (RNG) is a device designed to generate a sequence of numbers or symbols that don‘t have any pattern. Hardware-based systems for random number generation are widely used. Methods for generating random results have existed since ancient times, including dice, coin flipping, the shuffling of playing cards, the use of yarrow stalks and many other techniques. [1, 2]. The many applications of randomness have led to many different methods for generating random data. These methods may vary as to how unpredictable or random they are, and how quickly they can generate random numbers. [1, 2].

Key generation [3] is the process of generating keys from random values in order to secure the communication. It helps to encrypt the data so that no third party can access that data. So, for that key is required which should be so strong that it make hackers so confused that no one can even predict the message. For that, random value through which key is generated have to be strong enough.

II. Literature Survey

The following algorithms are pseudorandom number generators:

- Blum Blum Shub
- Middle Square Method
- Inversive congruential generator
- ISAAC (cipher)
- Lagged Fibonacci generator
- Linear congruential generator
- Linear feedback shift register
- Mersenne twister
- Multiply-with-carry
- Well Equidistributed Long-period Linear
- Xorshift

These all above techniques are used to generate pseudorandom numbers which can be used for different purposes.

III. Proposed Work

In this paper, random numbers are generated with the help of congruence equations using Chinese Remainder Theorem [5]. As it is discussed before, are those equations which are of the form-

$$x \equiv a \pmod{b}$$

A. Algorithm

```
Step 1- Start
Step 2- for(i=1;i<=5;i++)
a[i] ← input any 5 values
b[i] ← input any 5 values, where b>a
Step 3- Now, for generating random numbers, always take set of 3 equations each time and swap them all in order to generate all possible sets of equations.
```

Step 4- Put these values into the equation

$$Xi = a(i) \bmod b(i)$$

Step 5- For generating random numbers “x”

$$xn = (N * bn+1 * bn+2) \% bn \equiv an \qquad (i)$$

In this proposed work, 5 equations have been taken, so for that firstly considered the equation with respect to which we have to compute the random numbers, as if, we have 5 equations from 1 to 5, then for first equation we will consider set of equations 2-3 and 4-5 and so on.

Then, from these two sets of equations, we will put the values of b’s according to equation (i). From this, number of pseudorandom numbers will be generated. After that, equations can be swapped to generate more pseudorandom numbers.

B. Example

Let us take an example to understand this, in this we assume three congruence equations be:-

$x\equiv a1 \bmod b1$ (1)

$x\equiv a2 \bmod b2$ (2)

$x\equiv a3 \bmod b3$ (3)

[Note :- $a<b$]

To compute the random numbers, equations will be solved like below method-

i.e.

For equation (1)

$C*(b2*b3) \bmod b1\equiv a1$

For equation (2)

$C*(b3*b1) \bmod b2\equiv a2$

For equation (3)

$C*(b1*b2) \bmod b3\equiv a3$

Through above given equations random numbers can be easily generated and these generated random numbers can be used to generate keys in order to encrypt the messages for any cryptographic techniques like in key distribution center, Diffie-Hellman key exchange, etc.

C. Features Of Proposed Scheme

i. More pseudorandom numbers generated at a time
ii. Simple coding
iii. can be used in any encryption scheme
iv. Easy to Analyze
v. Fast Response.
vi. Long-period random number sequence
vii. Unpredictability

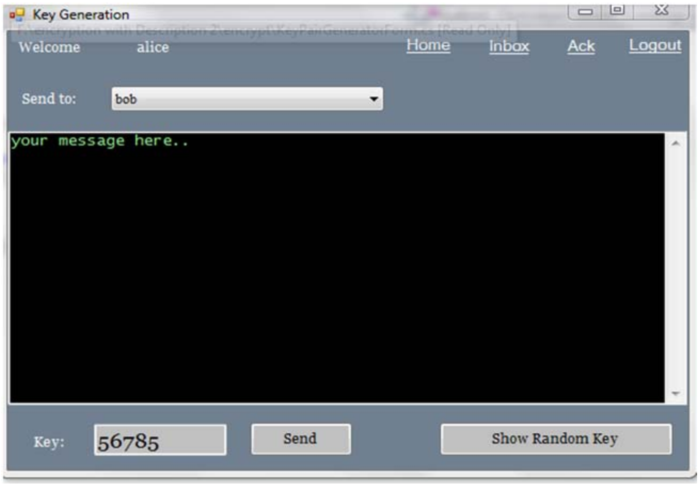
IV. IMPLEMENTATION

As discussed earlier, these random numbers can be used in many cryptographic applications in the form of secret key, as nonce, as cryptographic keys, as session keys and many more.

In this paper, these random numbers generated are used as a secret key between both the parties for secure communication. Without this generated random number, data will not decrypt.

When any user/sender wants to send any message to receiver, then at that time along with the message sender has to insert a 5-digit secret code, along with the message which will be encrypted through RSA key. The random number which will be used at encryption time will generate a random number which will be used later at decryption time.

As shown in below fig-1, in this, along with message, a secret key will be used for encryption purpose.



Welcome alice

Send to: bob

your message here..

Key: 56785

Figure-1 Encryption Process with the help of secret key

The random number which is used as secret key or a 5-digit code which is used will be here will be used to generate random numbers, and all these random numbers will be combined to form a unique string of random numbers.

As this is only 5 digit code, so these 5 digits will become the values for’ a’, and as ‘a’ must be less than b, so here, ‘b’ will become

$$b[i]= a[i]=2$$

So, from this, both the values for ‘a’ and ‘b’ will be filled and random numbers will generate.

Now, these all i.e 5-digit code, string of random numbers and message will be saved in an encrypted form.

When the receiver wants to open the message sent by the sender, the receiver will click for decryption, due to which all the data saved will start decrypting one by one. And when that 5-digit code or secret key used by sender will decrypt, it will generate string of random numbers with the help of proposed algorithm**,** which will be then matched with the random number generated at the encryption time. If both the strings will match, then the data will be decrypted. In this, secret key also helps to provide authentication and confidentiality. Here, this random number will also work as an acknowledgement between both the parties,

V. CONCLUSION

Proposed work has defined the generation of random numbers in a different way with the help of congruence equation. Random numbers generated may have less complexity then other existing techniques. These random numbers can be used for the simple encryption and decryption process as well as the digital signature technique also for the key distribution techniques etc.

REFERENCES

[1] P PAVAN KUMAR,"A new method for generating key for cryptography using Deterministic random number generator," International Journal of Engineering Trends and Technology (IJETT) – Volume 4 Issue 9- September 2013.

[2] Juan Soto," Statistical Testing of Random Number Generators," (301) 975-4641.

[3] *Dr. Mrs. Saylee Gharge et al,"*Percon8 Algorithm for Random Number Generation," *Int. Journal of Engineering Research and Applications* www.ijera.com *ISSN : 2248-9622, Vol. 4, Issue 5(Version 1), May 2014, pp.54-60.*

[4] Amrita Sahu," Proposed Method of Cryptographic Key Generation for Securing Digital Image," International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 10, October 2012 ISSN: 2277 128X.

[5] Tony Thomas,Sabu Emmanuel, Peng Zhang,"An Authentication Mechanism Using Chinese Remainder Theorem for Efficient Surveillance Video Transmission," 2010 Seventh IEEE International Conference on Advanced Video and Signal Based Surveillance