Analysis of Cryptography and Pseudorandom Numbers

Richa Agarwal

Student, M. Tech., Computer Science, Invertis University, Bareilly, India

Abstract: With the beginning of the use of internet, emergence of various e-commerce applications, social networks and many other organizations becomes the major source of data generation, which also requires security as it may contain some sensitive data. But today, data security is the major issue for safe transmission of data over the internet. As the number of users increases over the internet, the chances of cyber-crimes also increase. In that case, pseudorandom numbers plays an important role for safe data transmission. Different researches are done where random numbers are used in cryptographic applications for secure data communication.

Keywords: Cryptography, Pseudorandom Number, Encryption, Decryption

I. INTRODUCTION

In today's scenario, internet is widely used all over the world regularly, which is mostly use for data transmission which requires high security for communication without the involvement of any unauthorized user. In that case pseudorandom numbers are used for secure communication which can be used in many forms like in generating encryption keys, nonce, etc. These generated pseudorandom numbers can be applied in cryptographic applications for secure communication.

Cryptography [1] is the art of converting plaintext into secret code or converting data from readable text to unreadable text. Cryptography is closely related to the disciplines of cryptology and cryptanalysis where cryptology is the techniques for ensuring the secrecy and/or authenticity of information and cryptanalysis is what the layperson calls "breaking the code." In cryptography, there are two techniques for converting data from one form to another, i.e., encryption and decryption. In encryption, ordinary data (called plaintext) is converted into unintelligible form (called cipher text). In decryption, it is just the reverse of encryption, i.e. converting unintelligible form of data back to plaintext as shown in figure-1.

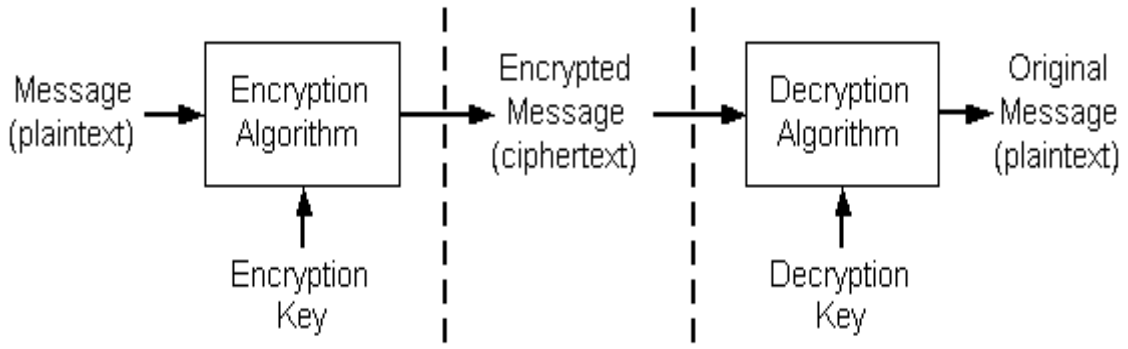

Figure-1: Encryption-Decryption Process

Pseudorandom numbers [2] are all different from each other and its main aim to provide authenticity. A common and an easy way to generate random numbers rely on cryptographically secure pseudorandom number generators. These are used for different approaches and computed by applying some mathematical computations so that they can't be recognized by any other third party who is not authorized and may be an eavesdropper. In this field, various researches have been done to generate efficient pseudorandom numbers.

II. CRYPTOGRAPHIC TECHNIQUES

In cryptography, there are two main cryptographic schemes [3].

A. Secret Key Cryptography

In this, a single key is used for both encryption and decryption. As shown in Figure-3, i.e. both the sender and receiver will use a single key 'K' for encrypting and decrypting the data. Let the sender A wants to send the message M to receiver B, so for that sender A will use the key 'K' to encrypt the plaintext and send that ciphertext 'C' to receiver. Then the receiver apply that same key 'K'(or ruleset) for decrypting the received ciphertext 'C' and recovers the plaintext from that. As in this, only a single key is used for encryption and decryption, that's why it is also called symmetric encryption. But in this approach, the biggest challenge is the distribution of key, as it must be known to both sender and receiver only and which should be secret. Algorithms for symmetric key cryptography are Data Encryption Standard(DES) and Advanced Encryption Standard(AES).

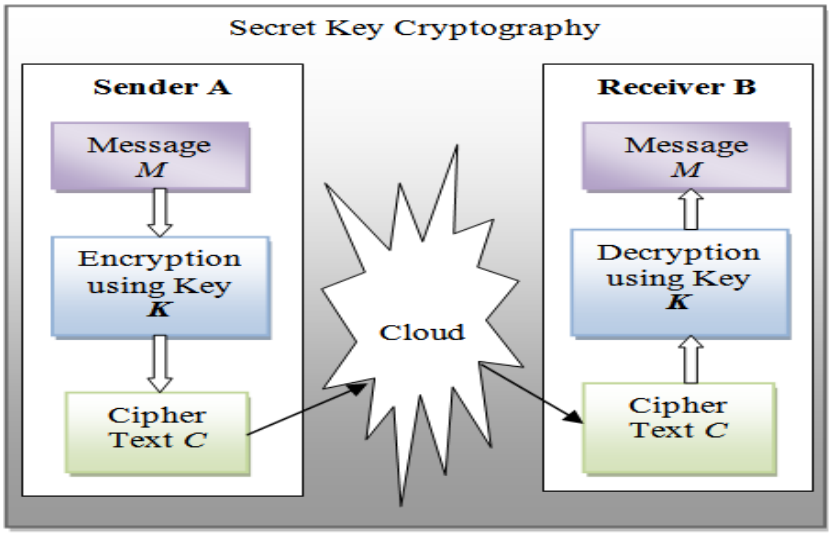

Figure 2: Secret Key Cryptography

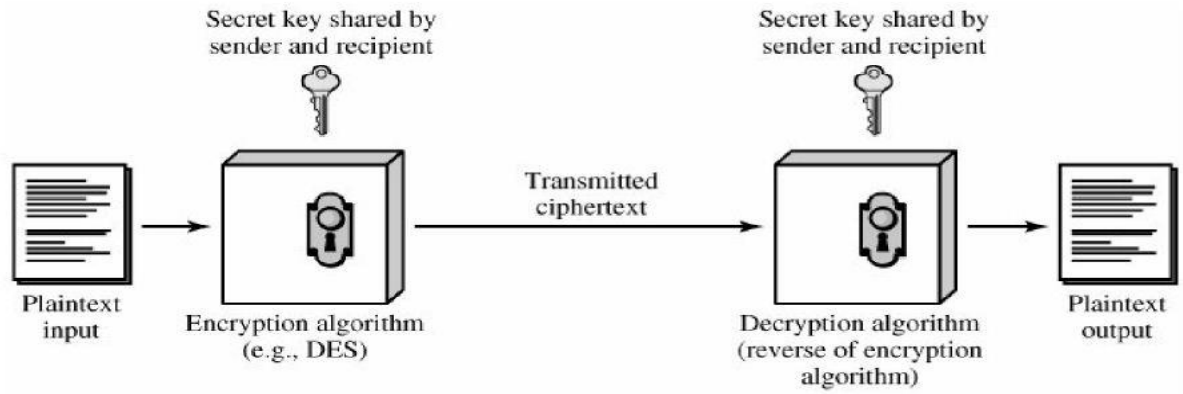

Figure 3: Data Encryption Standard

B. ***Public-Key Cryptography***

Public-Key Cryptography [6] is a form of cryptosystem in which two different keys are used for encryption and decryption in which one is a public key and one is private key and both these keys are mathematically related to each other.

As shown in Figure-5, sender *A* uses the public key of receiver *B* (or some set of rules) to encrypt the plaintext message *M* and sends the cipher text *C* to the receiver. Then, the receiver applies its own private key (or rule set) to decrypt the cipher text *C* and recover the plaintext message *M*. Because pair of keys is required, this approach is also called ***asymmetric cryptography***. Algorithms used in public key cryptography are RSA, Digital Signature Standard (DSS), Diffie-Hellman Key Exchange**.**

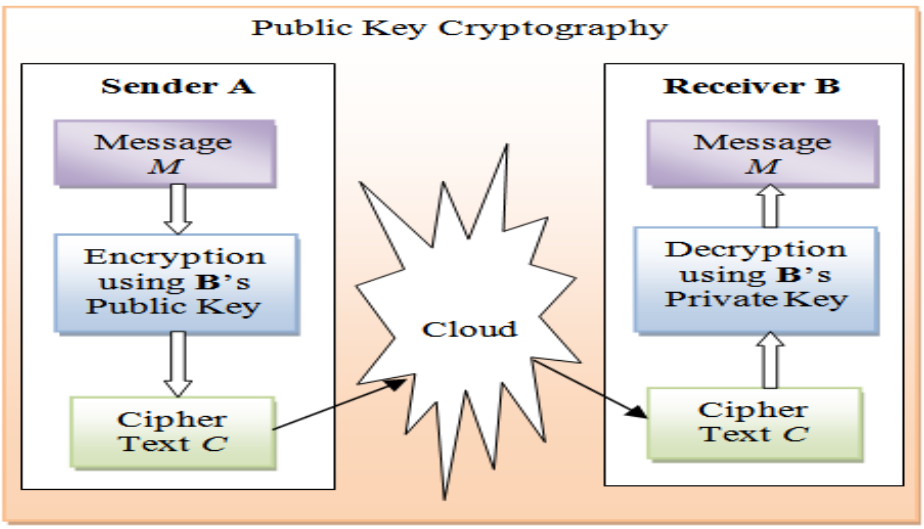

Figure 4: Public Key Cryptography

III. PSEUDORANDOM NUMBERS GENERATOR

Pseudorandom numbers [2] are important in many fields like in simulations, cryptography, gambling and gaming. Random numbers can be categorized into two categories namely true random numbers and pseudorandom numbers. True random numbers are those which uses an unpredictable physical means to generate numbers and Pseudorandom numbers use mathematical algorithms.

Some of the popular pseudorandom number generators are as follows-

C. ***Blum-Blum-Shub***

the Blum-Blum-Shub (BBS) generator [4] is a pseudorandom number generator which is proposed in 1986 by Lenore Blum, Manuel Blum and Michael Shub. This generator works on the form Xn+1 =Xn2mod M

where $M = p*q$ (product of two large primes i.e. p and q) .After each step, an output is derived from $xn+1$. The generated output is either parity bit or more of the least significant bits of $xn+1$.In this, a seed value is used which should be an integer and also co-prime to M but should not be 1 or 0 and the two primes used above i.e. p and q should both be congruent to 3 (mod 4).

D. ***Linear Congruential Generator***

Linear Congruential Generator (LCG) [5] used to generate sequence of pseudorandom numbers. It works on the following eqtn $Xn+1 = (aXn + b \bmod m)$ where a is called the multiplier, b the increment, and m denotes modulus. The outputs generated will follow the sequence: $X0;X1;X2; : : :$, where $X0$ should be given in advance called *seed*.

In this, a, b, m and $X0$ are the parameters of an LCG and the quality of LCG depends on the basis of selection of its parameters.

E. ***Mid-square method***

Mid-square method [6] initially starts with an initial number which is also known as seed and then that value is squared and the middle digits of this square become the random number after placement of the appropriate decimal. The middle digits are then squared to generate the second random number. This process is repeated until the required number of random numbers is generated.

F. ***Linear Feedback Shift Register***

A linear feedback shift register (LFSR) is a shift register whose input bit is a linear function of its previous state. The only linear function of single bits is xor, thus it is a shift register whose input bit is driven by the exclusive-or (xor) of some bits of the overall shift register value. The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current (or previous) state.

Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle.

*G. **Mersenne Twister***

The Mersenne twister is a pseudorandom number generator developed in 1997 by Makoto Matsumoto and Takuji Nishimura that is based on a matrix linear recurrence over a finite binary field $F2$. It provides for fast generation of very high quality pseudorandom numbers, having been designed specifically to rectify many of the flaws found in older algorithms.

Its name derives from the fact that period length is chosen to be a Mersenne prime. There are at least two common variants of the algorithm, differing only in the size of the Mersenne primes used. The newer and more commonly used one is the Mersenne Twister MT19937, with 32-bit word length. There is also a variant with 64-bit word length, MT19937-64, which generates a different sequence. For a k-bit word length, the Mersenne Twister generates numbers with a uniform distribution in the range $[0,2k-1]$.

Through pseudorandom number generation secrecy can be easily provided to data. As it can be used for generating encryption keys through which original data can be encrypted and converted into ciphertext 'C'. These can be generated by using any random number generation technique or by making own technique to generate such numbers which can't be easily recognized by anyone other than sender and receiver. These pseudorandom numbers are used in various techniques in different ways for secure communication.

IV. CONCLUSION AND FUTURE WORK

As security is one of the major concerns for everyone. Secrecy is required by everyone for secure data communication. For that pseudorandom numbers plays an important role in such conditions. They can be used as encryption keys to encrypt the data and make it secure to transmit from one to another. They are used in various cryptographic applications in different ways in order to protect the data. In future, it is possible of generation of different techniques of pseudorandom number generation other than present techniques.

ACKNOWLEDGMENT

I want to thank my guide and my parents for comments that greatly improved the paper.
Conflict of interest: I declare that I have no conflict of interest.
Ethical statement: I declare that I have followed ethical responsibilities.

REFERENCES

[1] Shyam Nandan Kumar (2015). Review on Network Security and Cryptography. International Transaction of Electrical and Computer Engineers System, 3(1), 1-11.
[2] Schaathun, H. G. (2015). Evaluation of splittable pseudo-random generators. Journal of Functional Programming, 25, e6.
[3] Blum, L., Blum, M., & Shub, M. (1986). A simple unpredictable pseudo-random number generator. SIAM Journal on computing, 15(2), 364-383.
[4] Li, C. C., & Sun, B. (2005, March). Using Linear Congruential Generators for Cryptographic Purposes. In Computers and Their Applications (pp. 13-19).
[5] K. Meenakshi Sundaram, T. Santhanam, M. Saroja and C.P. Sumathi (2010). A Performance Analysis of Modified Mid-Square and Mid-Product Techniques to Minimize the Redundancy for Retrieval of Database Records. Journal of Computer Science 6 (4): 386-391.
[6] Vikas Agrawal, Shruti Agrawal, Rajesh Deshmukh .Analysis and Review of Encryption and Decryption for Secure Communication. Inter. J. of Scientific Engineering and Research, Vol.2 (2)

