International Journal of Mathematics And its Applications
Volume 5, Issue 4–B (2017), 205–209.
ISSN: 2347-1557
Available Online: http://ijmaa.in/

International Journal of Mathematics And its Applications

Random Number and Combination Based Encryption and Decryption

Research Article

Sneha K. Patel[1]*

1 Department of H & S.S, Shree Swami Atmanand Saraswati Institute of Technology, Surat, Gujarat, India.

Abstract: For secure communication, cryptography has been used for thousands of years. Encryption and decryption are the process of transforming plaintext into the ciphertext and vice versa. There are three types of encryption and decryption algorithms exist which are classified as symmetric key cryptography, asymmetric cryptography algorithm and hash function. This paper presents an algorithm for data encryption and decryption which is based on random number generation, combination and MOD operation. This algorithm uses random number and combinations, generate a key to encrypt or decrypt the data.

Keywords: Encryption, Decryption, Random number, MOD operator, Symmetric key cryptography.

1. Introduction

Mathematics and numbers are weaved in every phase of our life. With the rapid growth of computational powers and availability of modern sensing, analysis and interpretation equipment computers are becoming more and more intelligent. So security means cryptography is being the most essential part of technology. Cryptography originated from the Greek word meaning "Secret Writing". It has a wonderful history from thousands of years. Cryptography is the study of mathematical techniques. One of them is Random Number Generation, which is a crucial component for the security of cryptographic systems for key generation. There are three types of encryption and decryption algorithms (cryptography algorithm) which are classified as symmetric key cryptography, asymmetric cryptography algorithm and hash function. Here I have discussed symmetric key cryptography which are jumble numbers uses the same key for encryption and decryption. Introducing some common terms which are used during this paper. These can be found in Schneier [1], Stallings [4] or any book of elementary Cryptography.

Cryptography: Science of top secret writing where one can store and transmit data in the hidden form to the intended individuals.

Key: A key is a piece of information (a parameter) and a sequence of bits and instructions which performs encryption and decryption. The algorithm would have no result without a key.

Plain text: Data in original form which is referred as clear text.

Cipher text: Encrypted data is called as cipher text.

Encryption: Encryption converts plaintext into ciphertext using mathematical function (key).

* *E-mail: patelsk2010@gmail.com*

Decryption: Decryption is the inverse (reverse) process of encryption.

In mathematically cryptography is defined as follows [2]: A cryptosystem is a five-tuple $(P,\ C,\ K,\ E,\ D)$, which satisfied the following conditions:

(1). P is a finite set of plaintexts.

(2). C is a finite set of ciphertexts.

(3). K is a finite set of keyspace.

(4). Each encryption function $e_k : P \to C$ and its corresponding decryption function $d_k : C \to P$ such that $d_k\left(e_k\left(x\right)\right) = x$ for every plaintext $x \in P$, $k \in K$, $e_k \in E$, $d_k \in D$.

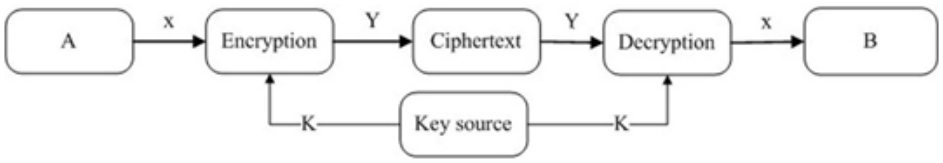

Figure 1. **The process of encryption and decryption.**

Suppose message is a string $X = x_1x_2\ldots x_n$. Sender A encrypted plaintext $x_i \in P$, $1 \leq i \leq n$ using the encryption function e_k specified by the predefined key K. A computes ciphertext $Y = y_i = e_k\left(x_i\right)$, $1 \leq i \leq n$, and sent to B. Now B receives $Y = y_1y_2\ldots y_n$, and decrypt it using the decryption function d_k, obtaining the original plaintext $d_k\left(e_k\left(x_i\right)\right) = X$. The process of encryption and decryption is as shown in Figure 1.

Congruences: Let m be a fixed positive integer. An integer a is congruent to an integer b modulo m if $m \mid (a - b)$. In symbols we write $a \equiv b\,(mod\ m)$.

Combinations: A selection of one or more things without regard of order.

There are many ways and categories of cryptographic algorithms which are based on the number of keys that works for encryption and decryption. There are three types of algorithms discussed by Gupta et. al. [3] and Stallings [4].

(1). **Symmetric Key Cryptography:** Symmetric (Secret) Key Cryptography is a single key used for encryption and decryption. With the use of key sender encrypt the plaintext into ciphertext and sends it to the receiver. The receiver applies the same key to decrypt the message to read the plaintext.

(2). **Public-Key Cryptography (PKC):** Public Key Cryptography has a key pair. One key is used to encrypt the plaintext and other key is used to decrypt the ciphertext. Both keys are required for encryption and decryption.

(3). **Hash Function:** Hash functions are an algorithm that converts plaintext into ciphertext without key.

2. Proposed Algorithm

In this paper, I have used a random number, combinations and modulus (MOD operator) as an invertible operator for encrypting the messages. The step by step mathematical procedure is given below. It is divided into three parts. (1). Key generation (2). Encryption (3). Decryption

(1). **Key generation:**

- Select random integer numbers a and b. Here a and b are long digit numbers.
- Calculate $n = ab$ where n is too large.
- Generate random integer value r $(0 < r < n)$ and A any integer value.
- Calculate $N = n_{C_r}$.

Thus we generate a key $(N,\ A)$ which is an essential for sender and receiver to communication. For hikers to identify a key is very tuff. Because N is depended upon n and r, and n is depended on a and b.

(2). **Encryption:** Person S (sender) wants to send a plaintext M to R (receiver). Using generated key $(N,\ A)$, he compute

$$C \equiv (M + A)\ \ mod\ N$$

And send ciphertext C to R (receiver).

(3). **Decryption:** R (receiver) received ciphertext C. Use generated key $(N,\ A)$ and decrypt C by

$$M' \equiv (C - A)\ \ mod\ N$$

Thus he gets an original message $M = M'$.

3. Experimental Result

Suppose person S (sender) and R (receiver) wants to secrete communication. So first generate key as follows:

(1). Select random integer numbers $a = 12,\ b = 8$.

(2). Calculate $n = ab = 96$.

(3). Generate random integer value $r = 18$ $(0 < r < n)$ and $A = 9$.

(4). Calculate $N = n_{C_r} = 1.36779e + 019$. Generated key $(N,\ A) = (1.36779e + 019,\ 9)$.

Convert each alphabet of plaintext M to an ASCII code. Apply encryption algorithm and obtained ciphertext C. Convert C into the printable characters ASCII range (32 to 126) with adjustment $C = \ mod\ (C,\ 95) + 32$ in MATLAB on each value of C. Finally convert ASCII code in character form which is the ciphertext C. Apply reverse process of encryption to obtained plaintext M. Process of encryption and decryption is shown in Table 1 using above generated key with plaintext "Hello".

Plain text M	H	e	l	l	o
Numeric text M	72	101	108	108	111
Encryption: $C \equiv (\mathrm{M} + \mathrm{A})\ \ mod\ N$	81	110	117	117	120
Ciphertext C in an ASCII code	113	47	54	54	57
Ciphertext C in printable characters	q	/	6	6	9
Decryption: $M' \equiv (C - A)\ \ mod\ N$	72	101	108	108	111
Plain text M	H	e	l	l	o

Table 1. **Process of encryption and decryption.**

The process of an encryption and decryption using a Symmetric Key Cryptography algorithm has been verified in MATLAB which gives better results. The input Message, Key (N, A), encrypted message and decrypted message are shown in Figure 2.

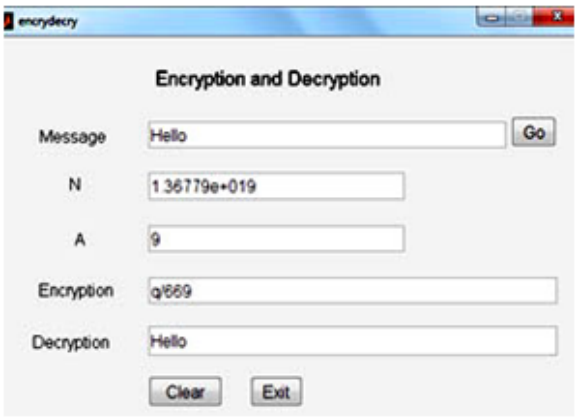

Figure 2. **Encryption and decryption process of input message in MATLAB.**

4. Advantages

- No one can break a generated key easily. Value of N depends on the values of a, b, r and A. Here r and A are random numbers.
- A key (N, A) must be known to communicate with each other.
- A hacker can not guess a value of key N or A easily as both depend on random numbers.
- Encryption and decryption operations are present in this algorithm which provides security.
- This algorithm works smoothly.

5. Applications

Security plays an important role in technology. Cryptography uses a variety of symmetric key encryption algorithms to provide security. Proposed algorithm is also used for the same. There are many places where we expect security like banks, militaries, crime branches, online communication, universities, E-commerce transactions, personal data, patients' medical data, private offices, government offices, organizations, digital signature and individual persons etc.. Thus this proposed algorithm is used at these places for confidentiality. It is used to encrypt confidential data, e-mails, messages, documents etc.. Encrypting File System (EFS) uses this algorithm for confidentiality. This algorithm is also widely used into the fields like Image processing, Image encryption and stenographic techniques.

6. Conclusion

Symmetric Key Algorithms have been developed by many researchers. This algorithm is very fast and secure for confidential communication because of its encryption and decryption process depends upon a key (N, A) which is used for security. As N is calculated with a combination of r $(0 < r < n)$ and n depends on random numbers a and b. Here A is also a random number.

References

[1] B.Schneier, *Applied Cryptography, Protocols, Algorithms and Source code in C*, John Wiley & Sons, Inc, (2001).

[2] D.R.Stinson, *Cryptography Theory and Practice*, CRC Press Inc, (1995).

[3] K.N.Gupta, K.N.Agarwala and P.A.Agarwala, *Digital Signature Network Security Practices*, PHI private limited, New Delhi, (2005).

[4] W.Stallings, *Cryptography and Network Security Principles and Practices*, Prentice Hall of India Private Ltd., New Delhi, (2005). .