International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 13, Number 4 (2017), pp. 537-545
© Research India Publications
http://www.ripublication.com

Information Security: New Cryptographic Approach

Sanjeev Gangwar
Department of Computer Application
V.B.S. Purvanchal University Jaunpur

Prashant Kumar Yadav
Department of Computer Science & Engineering
V.B.S. Purvanchal University Jaunpur

Abstract

In this era, human beings are becoming more powerful because of their ability to share their knowledge and information with each other, though they are very far geographically. This becomes possible only with the help of some communication network, and this network is shared to all. Now, the most important issue that will arise is the security of those knowledge and information from them who are sharing the communication network but not assumed to know that information. So, here we are proposing a method to hide our information from whom it is not supposed to know, even if those can capture hidden form of knowledge.

The term **Cryptography** is used to achieve security of information with the help of some algorithms, known as **Cryptographic Algorithm.** Now-a-days, there are basically two types of cryptographic algorithms are used as : Private key Cryptography and Public Key Cryptography. Here we are proposing a new private key cryptography, that will be very useful for information security.

Categories & Subject Descriptor:

[Cryptography & Network Security]: A New Cryptographic Algorithm.

Keywords: Information Security, Cryptography: Symmetric & Asymmetric.

1. INTRODUCTION

Now-a-days, the world wide communication media, Internet provides more convenient way to the peoples to communicate, although they are far away with each other. Internet is a widely used network which is shared to all. Hence security is going very important issue, if we are using Internet to communicate sensitive data and information.

There are different methods and techniques are provided to perform secure communication. One of those are Cryptographic algorithms. The cryptography is considered as the branch of both Computer Science and Mathematics. Cryptography is an art of insuring security and is a study of securing or hiding information. Cryptography is widely used in current technological applications such as ATM transaction, Internet Banking and many more. Currently due to demonetization of old currency, the Indian economy is going towards cashless, where different technologically advanced application will take place, which all will be cryptographically armed for insuring confidentiality and security. The security of information is preserved with the help of cryptographic algorithms.

The cryptographic algorithms are categorized into two types as: Private Key Cryptography sometimes known as Symmetric Key Cryptography, and Public Key Cryptography, also known as Asymmetric Key Cryptography. Here we are proposing an algorithm which is symmetric key cryptographic algorithm for securing information which is to be transmitted over insecure communication channel.

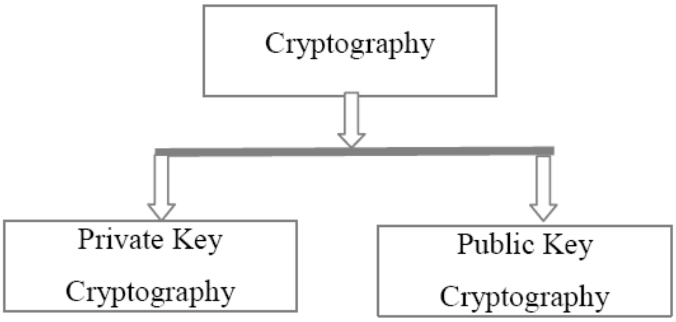


Fig. 1. Types of Cryptography

2. CRYPTOGRAPHIC ALGORITHM

The step by step procedures followed to ensure security of information is known as cryptographic algorithm. All these algorithms work in two phase as: Encryption phase and Decryption phase. The information that can be read and understand easily without any special effort is known as plain text. The process of converting plain text into unreadable form to hide and secure information is known as encryption and hidden form of information is known as cypher text. The process to gain back plain text from cypher text is known as Decryption. All these encryption and decryption processes are used to achieve the following goals:

2.1 AUTHENTICATION

This term is used to identify or authenticate both the peer entity that is supposed to receive information and the data origin entity from where the information is to be send. Digital signatures and digital certificates are used to provide authentication.

2.2 ACCESS CONTROL

The prevention of unauthorized use of resources is termed as access control. Access control mechanism allows only authenticated users to use information or resources.

2.3 DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure is called data confidentiality. There are four levels of data confidentiality as:

2.3.1 CONNECTION CONFIDENTIALITY

The protection of all user data on a single connection is known as connection confidentiality. The whole connection is made confident in connection confidentiality. Data must be sent via that confident connection to ensure confidentiality.

2.3.2 CONNECTIONLESS CONFIDENTIALITY

In this, the protection is performed on all user data in single data block and then can be transmitted over any connection.

2.3.3 SELECTIVE FIELD CONFIDENTIALITY

In selective field confidentiality, the protection takes place only on selected fields of information.

2.3.4 TRAFFIC FLOW CONFIDENTIALITY

The traffic flow confidentiality ensures confidentiality of the information that might be derived from observation of traffic flow.

2.4 DATA INTEGRITY

Data integrity is an assurance that the data which is received must be exactly same as sent by an authorized entity. Data integrity may be of different kind as:

- Connection Integrity with recovery, which detects any unauthorized modification on entire data sequence with recovery attempt.

- Connection Integrity without recovery, only detects unauthorized modification on entire data without recovery attempts.
- Selective-field connection integrity provides integrity for selected field within the user data with recovery attempt and without recovery attempts as per need.

2.5 NON REPUDIATION

The protection against denial by an entity or group of entities involved in a communication or having participated in all or part of communication, is provided by non-repudiation. Non repudiation can be provided on both, origin and destination end. It proofs that the message was sent by the specific entity as well as the message was received by the specific party.

All above discussed services are provided by both public key cryptography and private key cryptography. Here we are designing a new private key cryptographic algorithm, hence now we'll discuss about private key cryptography.

3. PRIVATE KEY CRYPTOGRAPHY

According to user's need, the private key encryption can be performed on both the block of data and the stream of data items, and hence the types of private key cryptography are:

i). Block Cypher and

ii). Stream Cypher.

Following figures show the encryption and decryption process of block cypher:

Encryption:

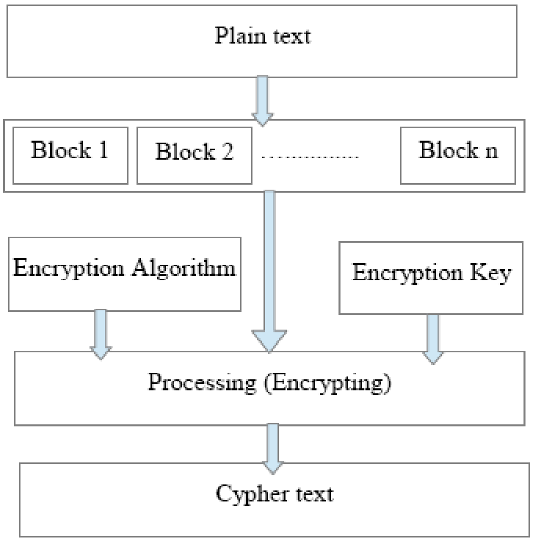


Fig. 3.1. Encryption process with Block Cypher

Decryption:

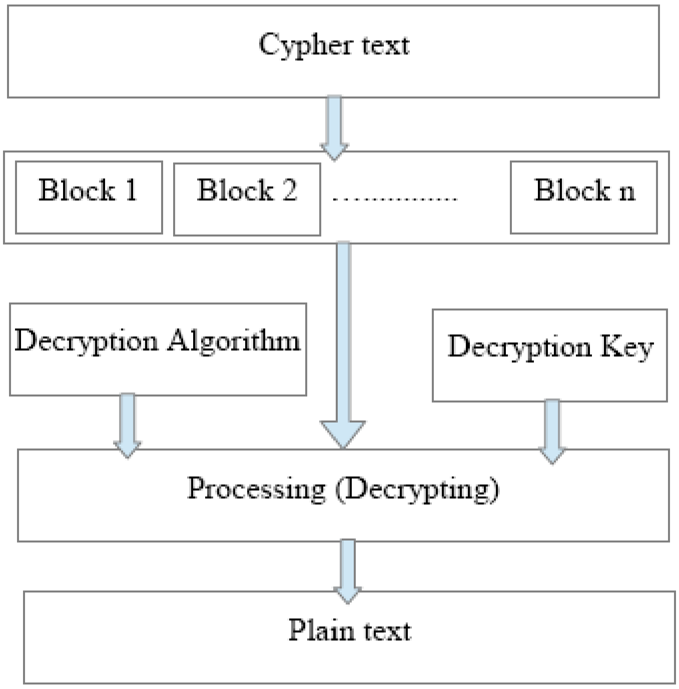


Fig. 3.2. Decryption process with Block Cypher

In block cypher, the encryption is performed on a block of data at a time with an encryption key and the same is used for encrypting next blocks of data. Block cypher uses same algorithm and key for encryption and decryption process. Block cyphers can be operated in several modes as:

i). CBC (Cypher Block Chaining)

ii). ECB (Electronic Code Book)

iii). CFB (Cypher Feedback) and

iv). OFB(Output Feedback).

In stream cypher, a stream of bits is encrypted using encryption key. In general, stream cypher operates bit by bit of plain text and produces cypher text. In stream cypher the encryption key changes constantly according to bits of plain text, and hence produces different cypher text every time for same plain text, but block cypher produces same cypher text for same plain text every time.

Following figures show the encryption process of stream cypher :

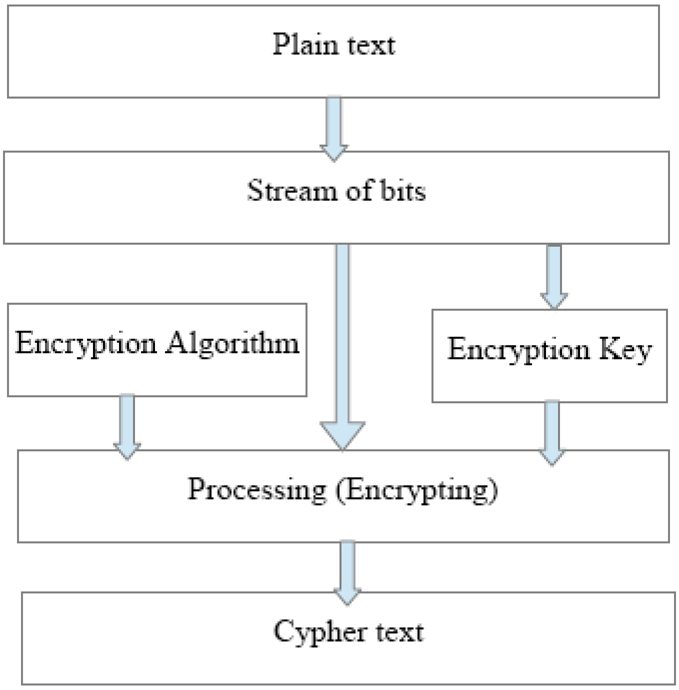


Fig. 3.3. Encryption process with Stream Cypher

There are two categories of stream cypher as:

i). Self-Synchronous stream cypher and

ii). Synchronous stream cypher.

In self-synchronous stream cypher, each bit in the keystream is calculated as the function of the previous n bits in the keystream. But in synchronous stream cypher, it generates the keystream in a fashion independent of the message stream but by using the same kestream generation function at both sender and receiver end.

Now-a-days, a number of other techniques and private key algorithms are used in the form of block cyphers as DES (Data Encryption Standard), which uses 56-bit key that can operate on 64-bit block. RC2 and RC5, Blowfish and Two fish are also the examples of such types of techniques. Here we are proposing a new technique which is symmetric in nature.

4. PROPOSED ALGORITHM (SYMMETRIC KEY CRYPTOGRAPHY)

This algorithm will work in two phases as:

i). Encryption phase and

ii). Decryption phase.

Encryption Phase:

1. Start
2. Input plaintext “ P ”.

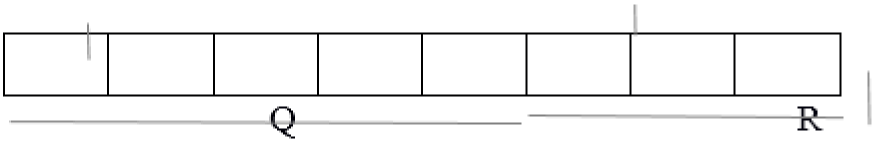
   where P = {alphabets, letters, special symbol, non-printable characters}
3. Write ASCII code “A” of each entity of plaintext.
4. Calculate “ A = B ”, where B = 8-bit binary number.
5. Calculate “ B = B’ ” , where B’ is the reverse of B.
6. Take a key “ K ” , where K is a 4-bit binary number and K>=1000.
7. Calculate

   Q = B’/ K .

   R = B’%K .

   Here, Q must be in 5 digit and

   R must be in 3 digit
8. Create 8-bit binary number “C” as,



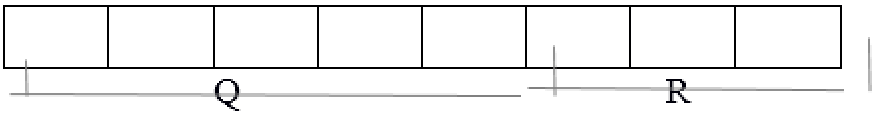
Here C is the desired Cyphertext.

9. End.

Decryption Phase:

1. Start
2. Input received Cyphertext “ C ” .
3. Assume Q = first 5-bit of C and

   R = Last 3 bit of C.



4. Take Previous encryption key “ K ”.
5. Calculate X = Q*K.
6. Calculate Y = X+R.
7. If

```
Y is not a 8-bit binary number
        Then
          make it 8-bit binary number by increasing
            0's in left hand side.
    Else
          Go to next step.
8.  Generate Y' = Reverse of Y.
9.  Write that entity E whose ASCII code is Y'.
10. Perform these operations for other 8-bit numbers to get other entities of plaintext.
11. Combine E's to get desired plaintext P.
12. End.
```

5. CONCLUSION

Proposed algorithm is used to encrypt sensitive information which is to be transmitted over insecure medium. This algorithm ensures confidentiality, integrity and other goals of cryptography, till the algorithm and key remains undisclosed. This algorithm works on very low cost and is very useful for small amount of data. However, it will work on large amount of data also. As we have seen that the key K is used for both the encryption and decryption process hence it will fall in the category of symmetric key cryptography.

The only drawback of this algorithm is that, if the algorithm and the key becomes known by the intruder, then the security of information will be compromised.

REFERENCES

[1] Ayushi, "**A Symmetric Key Cryptographic Algorithm**" International Journal of Computer Applications (0975 - 8887), Volume1, No.15, 2011.

[2] Vishwa Gupta, Gajendra Singh, Ravindra Gupta, "**Advance Cryptography Algorithm for improving Data Security**" International Journal of Advance Research in Computer Science and Software Engineering, Volume2: Issue 1, ISSN. No. : 2277 128X, January 2012.

[3] Shivangi Goyal "**A Survey on the Applications of Cryptography**" International Journal of Science and Technology Volume 1,No. 3, March, 2012**.**

[4] G. Julius Caesar, John F. Kennedy, **"Cryptography, Security Engineering"** an Article available at https://www.cl.cam.ac.uk/~rja14/Papers/SE-05.pdf

[5] Nigel Smart "**Cryptography : An Introduction (3rd Edition)**" an Article available at https://www.cs.umd.edu/~waa/414-F11/IntroToCrypto.pdf

[6] JNitin Jirvan, Ajay Singh, Dr. Sandip Vijay "**Review and Analysis of Cryptography Techniques**" International Journal of Scientific and Engineering Research, Volume: 4, Issue 3 , March, 2013, ISSN No. 2229-5518.