Journal Homepage: -www.journalijar.com
INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)
Article DOI:10.21474/IJAR01/5666
DOI URL: http://dx.doi.org/10.21474/IJAR01/5666

RESEARCH ARTICLE

DATA AND INFORMATION SECURITY: A MODERN CRYPTOGRAPHIC ALGORITHM.

Md. Obaidur Rahaman.
Assistant Professor, Department of Computer Science and Engineering, European University of Bangladesh, Bangladesh.

Manuscript Info

Manuscript History

Received: 19 August 2017
Final Accepted: 21 September 2017
Published: October 2017

Key words:-
Data andInformation Security, Cryptography: Private Key, Public Key, Stream Cipher, Block Cipher, CBC, ECB, CFB, OFB, Symmetric & Asymmetric.

Abstract

In this modern world, day by day people are becoming more powerful because of their ability to share their knowledge and information with each other, though they are very far away to each other destinations. 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 suggesting a method to hide our information from which it should not know, even if those can capture hidden form of knowledge.

The term Cryptography is used to provide information security using some algorithms known as Cryptographic Algorithm. At present, there are two types of cryptographic algorithms are used: private key cryptography and public key cryptography. Here we are proposing a new private key cryptography which will be very useful for information security.

Introduction:-

Today, throughout the world, the media, the Internet provides a more convenient way of communicating people, although they are far away from each other. Internet is a widely used network that is shared to all. Therefore, security is very important if we use the Internet to transmit sensitive data and information.

There are various methods and techniques are provided for secured communication. One of those are cryptographic algorithms. Cryptography is regarded as a branch of both computer science and mathematics. Cryptography is the art of security and the study of the protection or concealment of information. Cryptography is widely used in modern technological applications, such as ATM transaction, Internet banking and many others. Currently, due to the demonization of the old currency, the Bangladesh economy is moving towards non-cash settlements, where a different technologically advanced application will pass, which will be cryptographically armed to ensure confidentiality and security. Information security is preserved using cryptographic algorithms.

Cryptographic algorithms are divided into two types: cryptography of a private key, sometimes called cryptography with a symmetric key, and cryptography with a public key, also known as asymmetric key cryptography. Here we propose an algorithm that is a symmetric cryptographic key algorithm for protecting information that must be transmitted over an unsecured communication channel.

Corresponding Author:-Md. Obaidur Rahaman.
Address:-European University of Bangladesh, Bangladesh.

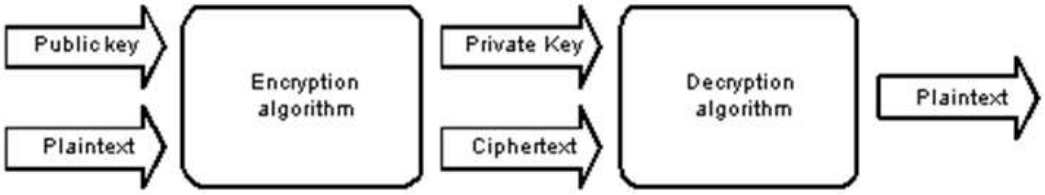


Fig. 1:-Types of Cryptography

Process Of Cryptographic Algorithm:-
Step-by-step procedures used to ensure the security of information are known as a cryptographic algorithm. All these algorithms work in two stages: the encryption phase and the decryption phase. Information that can be easily read and understood without much effort is called plain text. The process of converting plain text into an unreadable form for hiding and protecting information is known as encryption, and the hidden form of information is known as cipher-text. The process of obtaining a clean text from the text cipher is called decryption. All these processes of encryption and decryption are used to achieve the following goals:

Authentication:-
The sender and receiver can confirm each other's identity and the origin/destination of the information.

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.

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

Connection Confidentiality:-
The protection of all user data in an one connection is called connection confidentiality. All communication is confident in the confidentiality of communication. Data must be sent through this confident connection to ensure confidentiality.

Confidentiality Of Safety:-
In this case, protection is performed in all user data in a single data block, and then it can be transmitted over any connection.

Confidentiality Of Selective Field:-
With selective privacy of the fields, protection is provided only in selected areas of information.

Confidentiality Of The Flow Of Movement:-
The information cannot be understood by anyone for whom it was unintended.

Integrity:-
Data integrity is the belief that the data received should be exactly the same as those sent by the authorized person. The integrity of the data can be of different types:

1. Integrity of the connection with the recovery, which detects any unauthorized modification of the entire data sequence with the attempted recovery.
2. Integrity of connection without restoration, only detects unauthorized change of all information without attempts of recovery.
3. The integrity of the connection with the selective field ensures the integrity of the selected field within the user data with the attempted recovery and without attempts to restore it as needed.

Non Repudiation:-
Protection from refusal by a legal entity or a group of persons participating in the communication or participating in all or part of the message is provided by refusal of refusal. Continuity can be provided both at the end and at the end

of the goal. He confirms that the message was sent by a specific entity, and the message will be received by a specific party.

All of the above services are provided both with public key cryptography and private key cryptography. Here we are developing a new cryptographic algorithm with a secret key, so now we will talk about cryptography with a private key.

Type Of 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:
1. Block Cipher
2. Stream Cipher.

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

Encryption:-

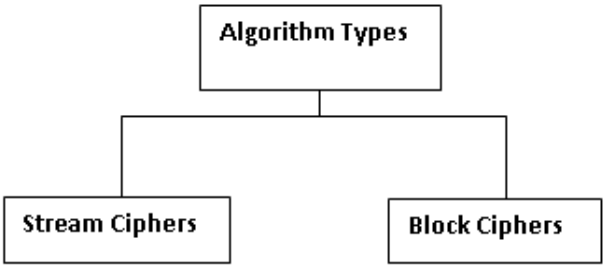


Fig.3.1. Types of Ciphers

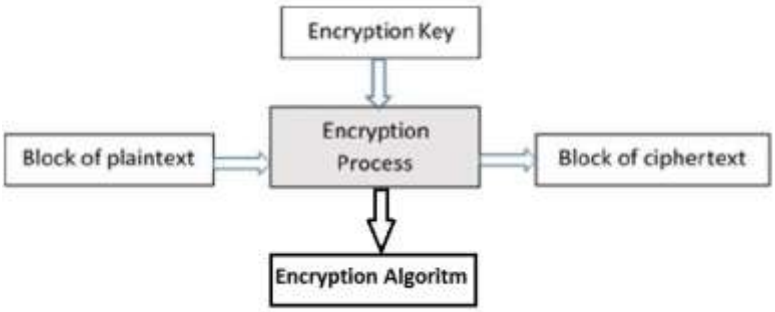


Fig.3.2:- Encryption process with Block Cipher

Decryption:

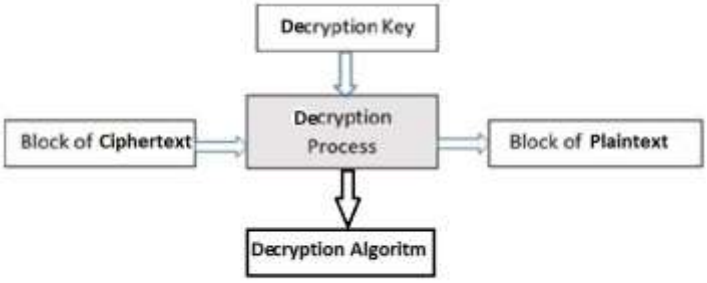


Fig. 3.3:-Decryption process with Block Cipher

Block Cipher:-

For Block cipher, the most important symmetric (meaning the same key is used for both encryption and decryption) algorithms are block ciphers. The general operation of all block ciphers is the same - a given number of bits of plaintext (a block) is encrypted into a block of ciphertext of the same size. Thus, all block ciphers have a natural block size - the number of bits they encrypt in a single operation. Block ciphers can be operated in several modes as:

1. CBC (Cipher Block Chaining)
2. ECB (Electronic Code Book)
3. CFB (Cipher Feedback)
4. OFB(Output Feedback).

CBC (Cipher Block Chaining): CBC is the most commonly using mode of operation for a block cipher. Prior to encryption, each block of plaintext is XOR-ed with the prior block of ciphertext. After decryption, the output of the cipher must then be XOR-ed with the previous ciphertext to recover the original plaintext. The first block of plaintext is XOR-ed with an initialization vector (IV), which is usually a block of random bits transmitted in the clear. CBC is more secure than ECB because it effectively scrambles the plaintext prior to each encryption step. Since the ciphertext is constantly changing, two identical blocks of plaintext will encrypt to two different blocks of ciphertext. CBC can be used to convert a block cipher into a hash algorithm. To do this, CBC is run repeatedly on the input data, and all the ciphertext is discarded except for the last block, which will depend on all the data blocks in the message. This last block becomes the output of the hash function.

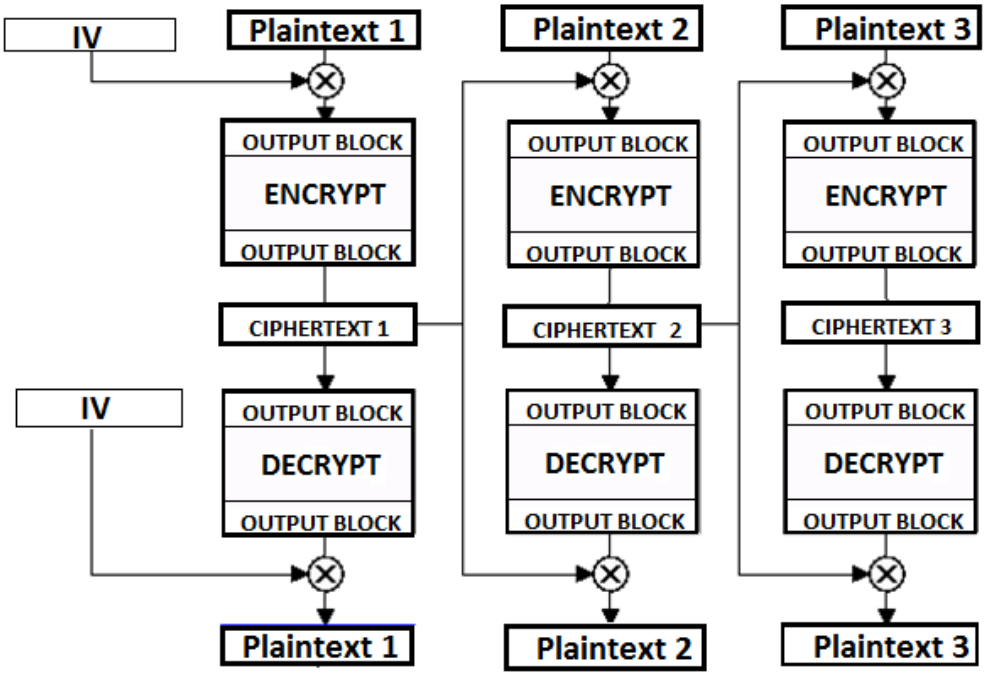


Fig. 3.4:- CBC (Cipher Block Chaining)

ECB (Electronic Code Book):-

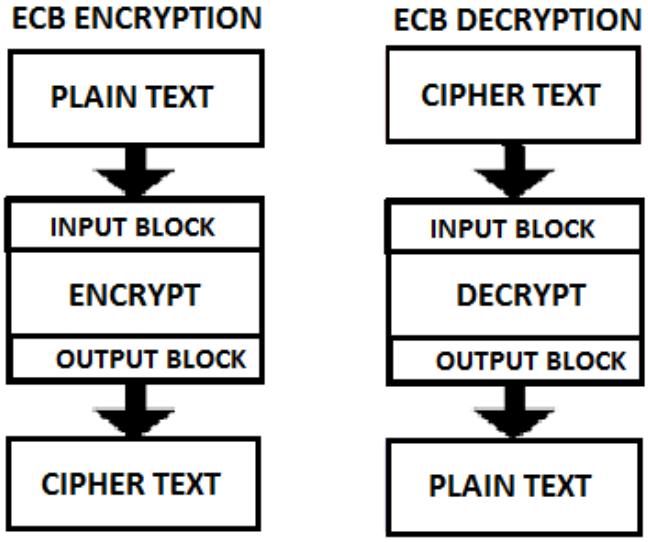


Fig. 3.5:-ECB (Electronic Code Book)

ECB is the simplest mode of operation for a block cipher. The input data is padded out to a multiple of the block size, broken into a integer number of blocks, each of which is encrypted independently using the key. In addition to simplicity, ECB has the advantage of allowing any block to be decrypted independently of the others. Thus, lost data blocks can not affect the decryption of other blocks. The disadvantage of ECB is that it aids known-plaintext attacks. If the same block of plaintext is encrypted twice with ECB, the two resulting blocks of ciphertext will be the same.

CFB (Cipher Feedback):-

The CFB mode is similar to the previously described CBC mode. The main difference is that one should encrypt ciphertext data from the previous round (so not the plaintext block) and then add the output to the plaintext bits. It does not affect the cipher security but it results in the fact that the same encryption algorithm (as used for encrypting plaintext data) should be used during the decryption process.

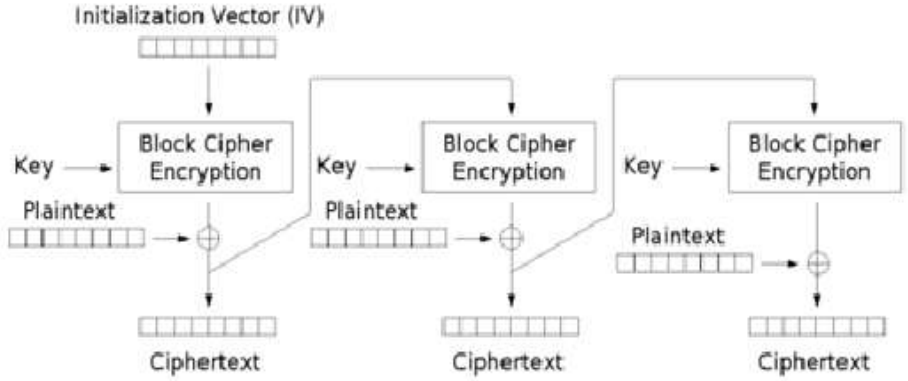


Fig.3.6:-CFB (Cipher Feedback)

OFB (Output Feedback):-

Output Feedback Mode (OFB) converts a block cipher into pseudo-random number generator. The output ciphertext is feed back into the input of the block cipher, and this process will be repeated to produce a stream of pseudo-random bits. The bit stream is completely determined by the algorithm, the key, an initialization vector, and the number of bits (k) feed back into the cipher during each step. The stream of bits can then be XOR-ed into the plaintext to produce ciphertext, effectively converting the block cipher into a stream cipher.

For the stream cipher, the bit stream is encrypted using an encryption key. In general, streaming cipher works bit by bit of plain text and creates cipher-text. In the stream cipher, the encryption key is constantly changing according to the plaintext bits and therefore, each time it processes different cipher texts for the same plain text, but the cipher block produces the same cipher each time for the same plain text.

Expression of the encryption process of streaming encryption:-

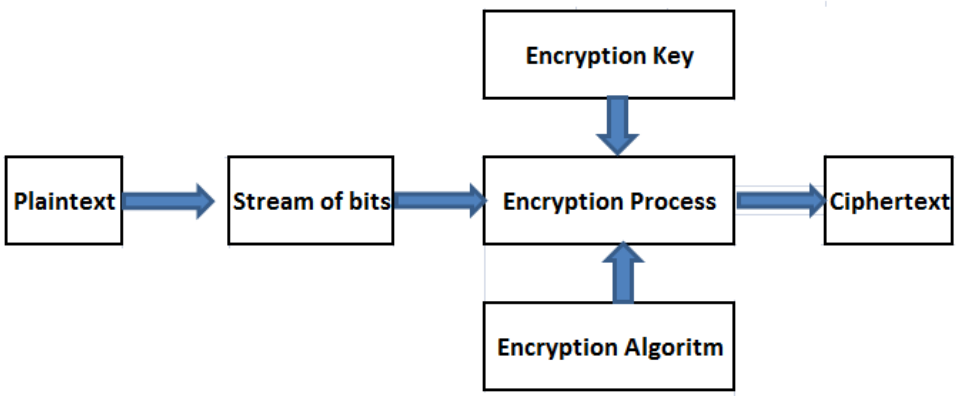


Fig. 3.7:-Encryption process with Stream Cipher

Types of stream cipher as:-
1. Self-Synchronizing stream cipher
2. Synchronizing stream cipher.

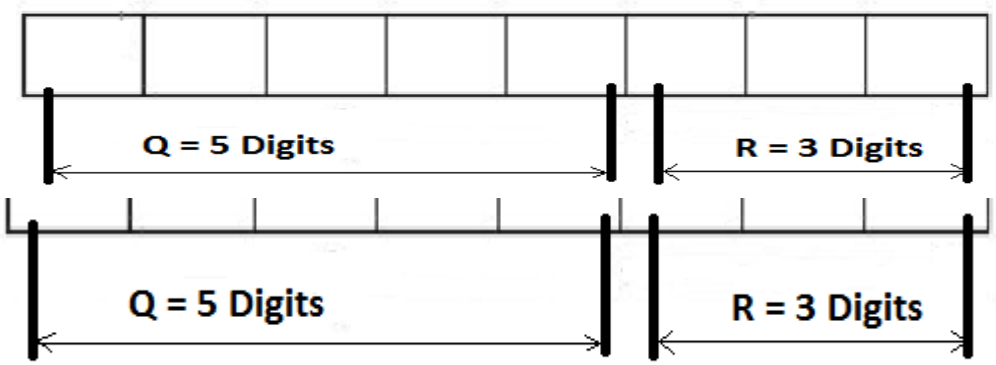
Self-Synchronizing and Synchronizing stream cipher:-
In a self- synchronizing stream cipher, each bit in the key stream is calculated as a function of the previous n bits in the key stream. But in a synchronizing stream cipher, it generates a key stream, regardless of the message flow, but using the same kestream generation function at both the sender's end and at the receiver.

Currently, a number of other methods and algorithms of private keys are used in the form of block ciphers as DES (Data Encryption Standard), which uses a 56-bit key that can work on a 64-bit block. RC2 and RC5, Blowfish and Two fish are also examples of such methods. Here we offer a new technique that is symmetrical in nature.

Proposed symmetric key cryptography algorithm-this algorithm will work in two stages or phases:
1. Encryption phase
2. Decryption phase.

Encryption Phase:-
1. Start
2. Input plaintext " P ".

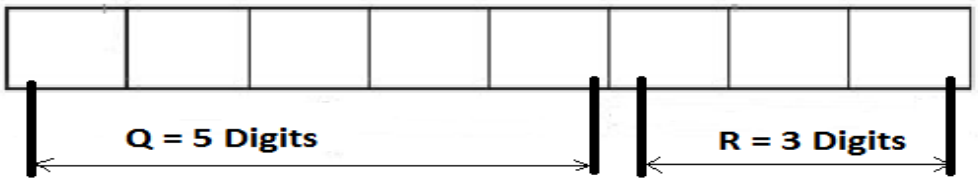
Where P = {alphabets, letters, special symbol, non-printable characters}
3. Write ASCII code "A" of each entity of plaintext.
4. Calculate " A = B ", where B = 8-bit binary number.
5. Calculate " B = B' " , where B' is the reverse of B.
6. Take a key " K " , where K is a 4-bit binary number and K >=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

Decryption Phase:-

1. Start
2. Input received Ciphertext“ 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
Thenmake 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.

Conclusion:-

The proposed algorithm is used to encrypt confidential information that must be transmitted over an insecure channel. This algorithm ensures the confidentiality, integrity and other purposes of cryptography until the algorithm and the key are disclosed. This algorithm works at a very low price and is very useful for a small amount of data. Nevertheless, it will work on a lot of data. As we have seen, the K key is used for both the encryption process and for decryption, hence it will be classified as a symmetric key cryptography.

The only drawback of this algorithm is that if the algorithm and the key become known to the attacker, then the security of the information will be violated.

References:-

1. Fundamentals of Computer Security, Springer publications "Basic Cryptographic Algorithms", an article available at www.itsc.state.md.us/oldsite/info/InternetSecurity/Crypto/CryptoI ntro.htm#Algorithms
2. Ayushi, "**A Symmetric Key Cryptographic Algorithm**" International Journal of Computer Applications (0975 - 8887), Volume1, No.15, 2011.
3. J. V. Shanta, "Evaluating the performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard) in IJCEM International Journal of Computational Engineering & Management", vol. 15, no. 4, **(2012)**, pp.43-49.
4. ShivangiGoyal "**A Survey on the Applications of Cryptography**" International Journal of Science and Technology Volume 1,No. 3, March, 2012**.**
5. G. Julius Caesar, John F. Kennedy, **"Cryptography, Security Engineering"** an Article available at https://www.cl.cam.ac.uk/~rja14/Papers/SE-05.pdf
6. "Introductionto Public-Key Cryptography", an article available at developer.netscape.com/docs/manuals/security/pkin/contents.htm.