ATLANTIS PRESS
Advances in Social Science, Education and Humanities Research (ASSEHR), volume 141
International Conference on Public Policy, Social Computing and Development 2017 (ICOPOSDev 2017)

Encryption and Decryption using Password Based Encryption, MD5, and DES

Hanna Willa Dhany
Informatics Engineering
University of Sumatera Utara
Medan, Indonesia
dhany.hanna@gmail.com

Fahmi Izhari, Hasanul Fahmi, Tulus, Sutarman
Informatics Engineering
University of Sumatera Utara
Medan, Indonesia
fahmiizhari@students.usu.ac.id, fahmijensen@gmail.com, tulus.ip@yahoo.com, sutarman@usu.ac.id

***Abstract*—Password-Based Encryption gets the encryption key from the password. To make the task from keyword to key is very time-consuming for an attacker, most implementations of Password-based Encryption will be combined with a randomization system, known as salt. It should be that we want to effectively select an encryption key. We may want to encrypt files based on the passwords we enter, so we can remember them. In this case, the only information would be a password. Password-Based Encryption is used in the application because usually the attacker repeatedly tries to guess undetected keywords and is beyond the original sender / recipient control, if the keyword is used to log in to the server, it can detect many possibilities that are not properly done and in the worst case is to shut down the server to prevent more effort, if a tapper take encrypted files that we use. Password Based Encryption with Message Digest (MD5) and Data Encryption Standard (DES) is a cryptographic method using algorithms that combine both hashing and standard encryption methods. MD5 was developed by Ronald Rivest where the MD5 takes messages of any length and generates a 128-bit message digest, and with the use of DES working in plaintext it is useful to return the same size ciphertext.**

Keywords— Cryptography, Encryption, Decryption, Password Based Encryption, MD5, DES.

I. INTRODUCTION

Technological developments are so rapid now, especially in the process of sending a message, but we often complain about safety. Security in data exchange is very important for users. This requires a mechanism for maintaining the authenticity of data in the exchange of data. As is the case in the data transmission many changes and the exchange of data made by irresponsible parties to take advantage. In sending messages through e-mail security is needed in order to maintain the integrity of the message.

For the example is hoax news case, where a person receives an electronic message from an incorrect news sender. It turns out that in the process of sending a message a change made by an irresponsible person who changed the message to sender incorrect information. In this case message security is necessary so that both parties do not feel disadvantaged, so the sender and the recipient must authenticate the message so that the two defendants can guarantee the source of the message.

Data security is always associated with cryptography. Cryptography is the study of how to maintain the security of a message and maintain the confidentiality of messages from irresponsibility by encoding into an unreadable form (chipertext). Cryptography studies mathematical techniques related to information security aspects such as confidentiality, data integrity and authentication. So the authenticity of the data can be guaranteed. Cryptography studies mathematical techniques related to information security aspects such as confidentiality, data integrity and authentication. So the authenticity of the data can be guaranteed.

The process that will be discussed in this paper include two basic cryptography process are Encryption and Decryption with the same key is used for both processes. The use of the same key for both encryption and decryption process is also called Secret Key, Shared Key or Symetric Key Cryptosystem. The Encryption process makes the message readable (plaintext) randomly unreadable (chipertext) then the Decryption process is the inverse of the encryption where this process will convert the chipertext into plaintext by using the same key. With the encryption and decryption process we will add the use of password-based encryption schemes in the protocol to implement symbolic and computational cryptography using symmetric, asymmetric, and password-based encryption. The usual alleged offline attacks can make consideration for the security process because the enemy makes every way to get any information about the passwords used. Therefore we make no exceptions to the possibility that the enemy may play a role, with the possibility of installing a standard active attack, and obtaining data from interactions with other participants. It is useful to integrate these results with a password-based encryption analysis now.

II. RESEARCH METHODS

A. Cryptography

Cryptography is a data security technique to ensure data confidentiality, in addition to cryptographic understanding is the study of mathematical techniques related to information security such as data confidentiality, data validity, data

integrity, data authentication (Hankerson et al., 2004)

B. Encryption and Decryption

Encryption is a process done to convert an undamaged message (plaintext) into an unreadable form (chipertext), decryption is a process done to convert an unreadable message into a readable and understandable form. The encryption and decryption process is governed by one or more cryptographic keys. Cryptosystem is a facility to convert plaintext to chipertext and vice versa. Based on the keys used for encryption and decryption, cryptography can be divided into symmetric key cryptography (Symmetric-key Cryptography) and asymmetric key cryptography (Asymetric-key Cryptography).
Encryption and decryption process can be seen in the picture

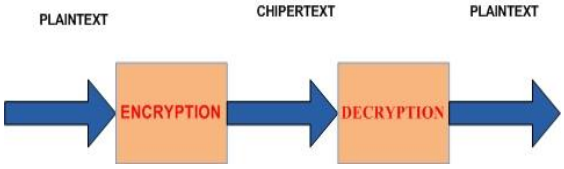

Figure 1.Encryption and Decryption Process

Cryptographic system or cryptosystem is a facility to convert plaintext to ciphertext and vice versa. In this system, the parameters that determine a particular involuntary transformation are called a set of keys. The encryption and decryption process is governed by one or more cryptographic keys. In general, the keys used for the process of encryption and description is not necessarily identical, depending on the system used. In general, the process of encryption and decryption operation can be explained mathematically as follows:

EK (M) = C (Encryption Process)
DK (C) = M (Decryption Process)

In the message M we declare be message C by using the key K, while in the decryption process we use the key K and do the message C that has been in the encryption and generate the initial message that is M.

C. Cryptography Algorithm

Symmetric Algorithms

Symmetric algorithms are cryptographic algorithm based on the key is divided into two namely the flow algorithm (Stream Cipher) and block algorithm (Block Cipher). In the Stream Cipher algorithm, the encoding process is oriented to one bit or one byte of data. While in the block algorithm, the encoding process is oriented to a set of bits or bytes of data. Examples of well-known symmetric algorithms are DES (Data Encryption Standard) (Silviana, 2013). The process of symmetric algorithm can be seen in figure 2.

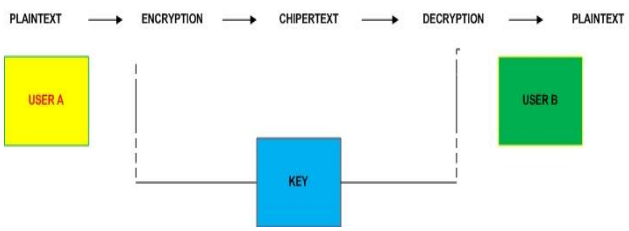

Figure 2. Symmetric Algorithms Process

This algorithm uses the same key for the encryption and decryption process. In a symmetric key cryptography system, the keys used for the encryption and decryption process are essentially identical, but one key can be derived from another key. These keys must be kept secret. Therefore this system is often referred to as a secret key cipher system.

Asymmetric Algortihms

Asymmetric algorithms are algorithm that uses different keys for encryption and decryption. This algorithm is often called a public key algorithm because the key for encryption is made public (Public Key) or can be known by everyone, but the decryption key is only known by the person authorized to know the data is encoded or often called the private key (Private Key). Examples of well known algorithms using asymmetric keys are ECC and RSA. The process of asymmetric algorithm can be seen.
A simple public key encryption process involves the following four stages:

1. Each user in the network creates a pair of keys to use as an encryption and decryption key of the message to be received.
2. User then publishes its encryption key by placing its public key into a public place. Other key pairs are kept confidential.
3. If user A wants to send data to user B, it will encrypt the data by using the user's public key B.
4. When user B decrypts data from user A, it will use its own private key. No other party can decrypt the data because only B alone knows the private key B.

D. Comparison of Symmetric Algorithms with Asymmetric Algorithms

Both Symmetric and Asymmetric Algorithms have their own advantages and disadvantages.
Excess symmetric key cryptography:

1. The symmetric cryptography algorithm is designed so that the encryption and decryption process takes a short time.
2. The size of the symmetric key is relatively short. A symmetric algorithm can be used to generate a random number.
3. A symmetric key algorithm can be constructed to produce a stronger cipher.

4. Authentication of direct data transmission is known from the received ciphertext, because the key is known only to the sender and the recipient only.

Symmetric key cryptography shortcomings:
1. Symmetric keys should be sent over a secure channel. Both communicating entities should maintain key secrecy.
2. The key must be changed frequently, perhaps every communication.

Advantages of asymmetric key cryptography:
1. Only private keys need to be kept confidential by every communicating entity. There is no need to send a private key as symmetric key cryptography.
2. Pairs of public keys need not be changed, even in long periods of time.
3. Can be used in the delivery of symmetric keys.
4. Some public key algorithms can be used to digitally sign members on data.

Asymmetric key cryptography shortcomings:
1. Data encryption and decryption are generally slower than symmetric cryptographic systems, because encryption and decryption use large numbers and involve large powers of operations.
2. The size of ciphertext is bigger than plaintext.
3. The key size is relatively larger than the symmetric key size.
4. Because the public key is widely known and can be used by everyone, ciphertext does not provide information about authentication of the sender.

E. Attacks on Cryptography

Each attack in cryptography of a cryptanalyst seeks to find the key or find the plaintext of the ciphertext with the assumption of cryptanalysis knowing the cryptographic algorithm used. According to Kerckhoff's principle all cryptographic algorithms must be public, only secret keys (Silviana, 2013).

The types of attacks in cryptography based on the attacker's involvement in communication:

1. Passive attack

The attacker does not engage in direct communication with the sender and recipient and only wiretaps to obtain as much data or information as possible.

2. Active attack

Attackers interfere with communication and influence the system to their advantage and attackers alter the flow of messages such as:
1. Delete a portion of ciphertext
2. Change the ciphertext
3. Inserting fake ciphertext
4. To reply the old messages

The types of attacks in cryptography are based on techniques used to find keys:

1. Exhaustive attack

Attackers use a way to find keys by trying all possible keys, surely manage to find the key if there is enough time.

2. Analytical attack

Attackers use the means by analyzing the weaknesses of cryptographic algorithms to reduce the possibility of unlikely keys by solving mathematical equations. This method is usually faster to find the key than the exhaustive attack. A cryptographic algorithm is said to be safe when it meets three of the following criteria:
1. The mathematical equations that describe the operation of cryptographic algorithms are so complex that the algorithm can not be solved analytically.
2. The cost to solve the ciphertext goes beyond the value of the information contained in the ciphertext.
3. The time it takes to break the ciphertext beyond the length of time the information must be kept confidential.

F. Hash Function

The H hash function is a transform that takes input with size m and returns a fixed-size string called a hash value h (where, h = H (m)). This simple hash function has many different types of computing utility, but when used for cryptographic issues, hash functions are always added with a number of additional properties (Liao & Shen 2006). What is needed for a hash cryptography function:
1. Input with any length
2. The result has a fixed length output
3. H (x) is generally easy to calculate for any value of x
4. H (x) is one way
5. H (x) never has any problem with others

The H hash function is a one-way function because it is difficult to invert which means for the hash value h, it is difficult to find the input value x satisfying the equation H (x) = h. The value of a hash function declares a message or a longer document originating from the computation process. This is interesting because with the hash function, we can create a digital fingerprint for a document. The best known examples of hash functions are MD2, MD5 and SHA. Perhaps a common use of hash cryptography is the creation of digital signatures. Since hash functions are generally faster than other digital signature algorithms, hash functions are more commonly used to derive a hash value function by calculating a signature that results in a smaller hash value than the document itself. In addition, the public may provide a suggestion or opinion without disclosing the content of the opinions contained therein. This method is used in assigning dates to a document where by using hash functions, each person can assign date to the document without showing the contents of the document during the date allocation process.

Cryptographic hash function is a hash function that has some additional security properties that can be used for data security purposes. A hash function is a function that efficiently converts a finite input string to an output string with a fixed length called a hash value.

The characteristic of a cryptographic hash function:

1. *Preimage resistant*

If it is known that hash value h is difficult (computationally not feasible) to get m where h = hash (m).

2. *Second Preimage resistant*

If m_1 input is known then it is difficult to find input m_2 (not equal to m_1) which causes hash (m_1) = hash (m_2)

3. *Collision-resistant*

It is difficult to find two different inputs m_1 and m_2 causing hash (m_1) = hash (m_2)

Some examples of cryptographic hash algorithms are MD4, MD5, SHA-0, SHA-1, SHA-256, SHA-512.

Encryption:

1. Plaintext is arranged into blocks m_1, m_2, ..., such that each block represents a value in the range 0 to p - 1.
2. Choose a random number k, in which case $0 \leq k \leq p - 1$, such that k is relatively primed with $p - 1$.
3. Each block m is encrypted by the formula :

$$a = g^k \bmod p$$
$$b = y^k m \bmod p$$

Set a and b are ciphertext for message blocks m.
So, ciphertext size is twice the size of the plaintext.

Decryption :

To decrypt a and b secret key, x, and plaintext m are recovered by equation:

$$m = b/a^x \bmod p$$

because :

$$a^x \equiv g^{kx} \pmod p$$

then :

$$b/a^x \equiv y^k m/a^x \equiv g^{xk} m/g^{xk} \equiv m \pmod p$$

Which means that plaintext can be recovered from the ciphertex set a and b.

G. Password Based Encryption

Password Based Encryption (PBE) is a symmetric cryptographic method that uses a password-like key to perform the encryption process and uses the same key to perform the decryption process so that it will generate the same data as the original plaintex data. Plaintex data that has been encrypted will produce a chipertex that can not be read by others. Chipertex is what will be sent to a second party so will have a reliable confidentiality. The resulting chipertex data will be changed according to the password data input provided. PBE cryptography is based on the hashing mechanism. A password and salt will be combined so that it will generate random data through the application function process and will be processed by the iteration count so that when the mixing process has finished it will produce the data in the form of chipertex.

H. PBE with MD5 and DES

PBE with MD5 and DES is a cryptographic method using the Message Digest 5 (MD5) and Data Encryption Standard (DES) algorithms. MD5 is the message digest algorithm developed by Ronald Rivest in 1991. MD5 takes messages of any length and generates a 128 bit message digest. On MD5 messages are processed in 512 bit blocks with four distinct rounds. DES, the acronym of the Data Encryption Standard, is the name of the Federal Information Processing Standard (FIPS) 46-3, which describes the data encryption algorithm (DEA).

DEA is also defined in ANSI standard X3.92. DEA is an improvement of the Lucifer algorithm developed by IBM in the early 1970s. Although the algorithm is essentially designed by IBM, the NSA and NBS (now NIST (National Institutes of Standards and Technology) play an important role in the final stages of development. DEA, often called DES, has been extensively studied since its publication and is the best known and most widely used symmetric algorithm. DES has a 64-bit block size and uses a 56-bit key lock during execution (8 bit parity removed from a 64 bit key). When used for communication, both sender and receiver must know the same secret key, which can be used to encrypt and decrypt messages, or to generate and verify message authentication code (MAC).

I. MD5 (Message Digest 5)

Message Digest 5 (MD-5) is one of the most widely used of one-way hash functions. MD-5 is the fifth hash function designed by Ron Rivest. MD-5 is a development of MD-4 where there is an addition of one round. MD-5 processes the input text into 512 bit bits of blocks, divided into 32 bits of sub-blocks of 16 pieces. The output of the MD-5 is 4 blocks of 32 bits each which will be the usual 128 bits called the hash value.

MD5's main node has a 512 bit long message block that goes into 4 rounds. The output of MD-5 is 128 bits from the lowest byte A and the highest byte D Each message will be encrypted, first searched how many bits are contained in the message. We consider as much as b bits. Here b is an integer non-negative bit, b can be zero and not necessarily multiples of eight.

Message Process in Block 16 Word

In MD-5 there are also 4 (four) nonlinear functions each used in each operation (one function for one block), is:

F(x,Y,z) = (x ρνY) ρν ((ρνx) ρνz)
G(x,Y,z) = (x ρνz) ρν (Y ρν (ρνz))
H(x,Y,z) = x ρνY ρνz
I (x,Y,z) = Y ρν (x ρν (ρνz))

Here can be seen one operation of MD-5 with the operation used as an example is FF (a, b, c, d, Mj, s, ti) showing a = b + ((a + F (b, c, d) + Mj + ti) <<<s). If Mj represents the j-message of the sub-blocks (from 0 to 15) and <<<s describes the bit will be shifted to the left as much as s bit, then the fourth operation of each round is:

FF (a, b, c, d, Mj, s, ti) showing a = b + ((a + F (b, c, d) + Mj + ti) <<< s)

GG (a, b, c, d, Mj, s, ti) showing a = b + ((a + G (b, c, d) + Mj + ti) <<< s)

HH (a, b, c, d, Mj, s, ti) showing a = b +

((a + H (b, c, d) + Mj + ti) <<< s)
II (a, b, c, d, Mj, s, ti) showing a = b +
((a + I (b, c, d) + Mj + ti) <<< s)

J. DES (Data Encryption Standard)

The most commonly used encryption scheme today is Data encryption Standard (DES). DES was adopted in 1977 by the National Bureau of Standards, now called the National Institute of Standards and Technology (NIST), as Federal Information Processing Standard 46 (FIPS PUB 46). In DES, data is encrypted inside 64 bit blocks using 56 bit keys. The DES algorithm converts 64 bit inputs in various steps to 64 bit outputs. The same step, with the same key, is used to decrypt the resulting ciphertext. In 1960, IBM started a project in computer cryptography led by Horst Feistel. The project was completed in 1971 with the development of an algorithm known as LUCIFER, which was sold to Lloyd's of London for use on the cash delivery system, which was also developed by IBM. LUCIFER is a block cipher that operates on 64 bit blocks, using a 128 bit key size. Due to the promising results, IBM later developed this system commercially. This effort is led by Walter Tuchman and Carl Meyer, and involves not only IBM, but also the technical consultants from the NSA. As a result, new versions of LUCIFER appear more resistant to cryptoanalyst but by reducing key size to 56 bits so that it can be implemented on the system with a single processor. Meanwhile, the National Bureau of Standards (NBS) in 1973 issued a request for national chiper standards. IBM sent the results of the Tuchman-Meyer proye. This is the best algorithm proposed and adopted as Data Encryption Standard.
DES works in bit models, or binary numbers 0 and 1. Each group of 4 bits forms a hexadecimal, or 16 based number. The binary number 0001 forms the hex numbers 1, and so on. DES works by encrypting each group consisting of 64 bits of data. To perform encryption, DES requires a key that also has a 64 bit size, but in practice the 8th bit of each group of 8 bits is ignored, so the key size becomes 56 bits. For example, if we want to encrypt the message "8787878787878787" with key "0E329232EA6D0D73", it will generate ciphertext "0000000000000000". If the ciphertext is decrypted using the same key, then the output is the original message. DES is a "block cipher", that is, DES works in plaintext with given size (64 bits) and returns ciphertext of the same size.

III. DESIGNING

In this application system encryption and encryption process with the method of PBE (password based encryption) with MD5 and DES done on the structure of applications that have been made, can be seen from the flowchart chart as follows:

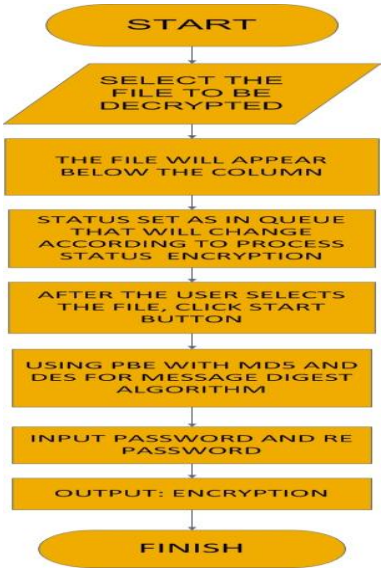

Figure 3. Flowchart Encryption

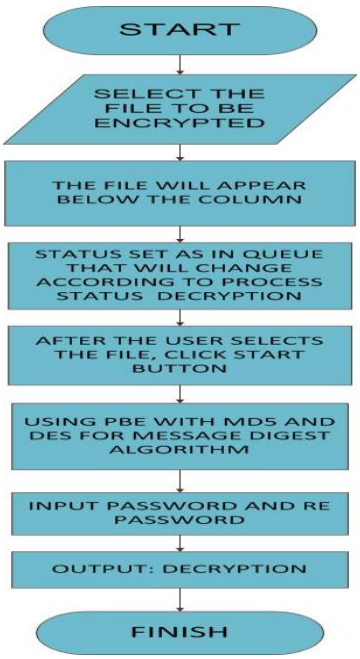

Figure 4. Flowchart Decryption

IV. RESULTS AND DISCUSSION

We must protect the files of others who will open them for bad interests. That's when I thought about encrypting my files and storing them on my harddrive. Even if someone wants to open it he should decrypt the file and then be able to open it.

Since I encrypt files using passwords and also hashes added, it's hard for anyone to decrypt them. Files can be added in the app to encrypt or decrypt in two ways. Either click the select button, choose the encryption key and will help the user to choose which files will be encrypted. Select the decryption key to help the user to select the encryption file. The application will generate an encryption and decryption file depending on which button will be selected. The app uses PBE with MD5, to enter the default Iteration hash password 100. How many times the hash password is determined by the iteration count. Enter a password to protect the file and be used for cryptography. Resetting a password must be exactly the same as the initial password to check if the password is the same as you want. When decrypting an encrypted file, the user needs the same Message Digest Algorithm, Hash Iteration and password used to encrypt the file. If the user provides an incorrect Message Digest Algorithm, Password Hash Iteration or Password when decrypting a file that does not match the Encrypted file, the application will prompt to re-enter the details, so that it can be correctly decrypted. At the moment Encryption password has to be provided for a file must be same for the file at the time of decryption. Encryption and decryption takes time depending on the size of the file to be processed. For example, if the file is 2 GB, it takes about 20 minutes to encrypt or decrypt the file.

Applications can be viewed with the following picture :

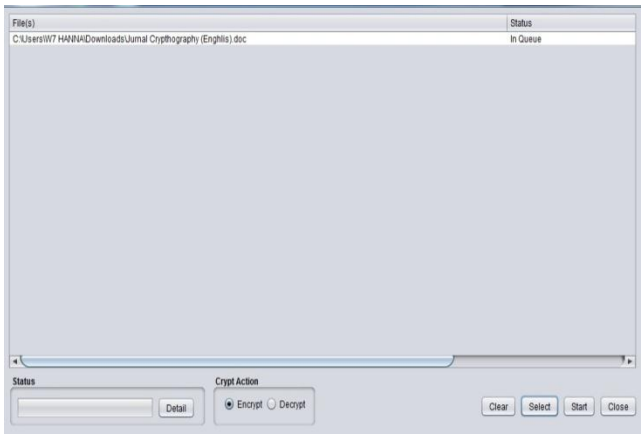

Figure 5. Selection Process Files to be encrypted or decrypted

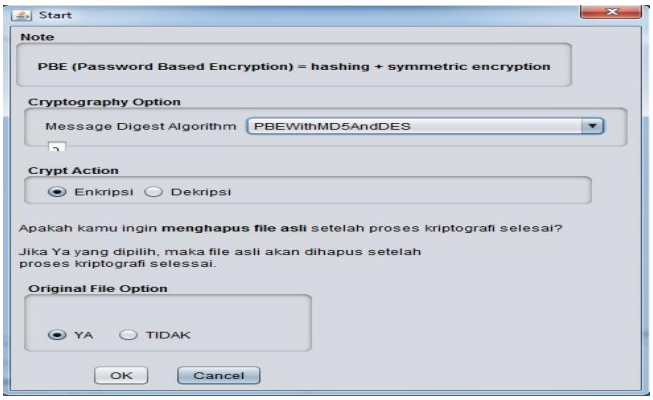

Figure 6. Encryption / Decryption Process in the form of a file

V. Conclusions And Suggestions

A. *Conclusion*

Applications that have been designed can generate encryption or decryption files, by obtaining the encryption key from the password. The technique generates the secret key of an artificial password called Password-Based Encryption and by using MD5 because it uses an algorithm that combines standard hashing and encryption methods as well as DES that works in plaintext useful for returning the same size chipertext. Password-Based Encryption = encryption hashing + 64-bit symmetric randomly added to password and hash using MD5.

B. *Suggestions*

The system is built based on the flow of the writer, then for better results and maximum required advice from any party to supplement the existing deficiencies. The author suggests the development of further research to security the message as follows:

- This application can be developed to create a message Encryption and Decryption using Affine Chiper, Caesar Chiper, etc.
- These applications can be developed using a better algorithm than the Password Based Encryption, MD5, and DES in anticipation of attacks by certain parties.

References

[1] Munir, Rinaldi., 2006, Kriptografi, Bandung, Informatika.
[2] Martin Abadi, Bogdan Warinschi, Password-Based Encryption Analyzed, Computer Science University of California, Standford University.
[3] Singh, S Preet and Maini Raman. “Comparison of Data Encryption Algorithm”, International journal of Computer Science and Communication, vol.2, No.1, january-June, pp. 125-127.
[4] Stallings W., 1999, Cryptography and Network Security Principles and Practice second edition. Prentice Hall, New Jersey, USA
[5] Stinson, D,; “Cryptography, Theory and Practice:; CRC Press; Second edition; 2000.