A Review on Symmetric Key Encryption Techniques in Cryptography

Mohammad Ubaidullah Bokhari
Dept. of Computer Science,
Aligarh Muslim University
Aligarh, India

Qahtan Makki Shallal
Dept. of Computer Science,
Aligarh Muslim University
Aligarh, India

ABSTRACT

In the era of digital communication, the information sharing is rapidly increased. All the data which being sent or received are vulnerable to many active and passive attacks. Therefore, secure the data during communication is the most important concern. Cryptography performs an essential role to secure the communication in network and it comes with an amazing solution to supply the needed protection against the intruders of data. Over a considerable time, the techniques of data encryption took a huge leap from very easy methods to very difficult mathematical calculations in an effort to generate a strong security for the communication. However still along with its difficulty, the algorithms of cryptographic are prone to many attacks. this paper is explains many techniques of symmetric key encryption, its comparison and their vulnerabilities to attacks.

Keywords

Cryptographic, cryptographic goals, Classical cryptographic, modern cryptographic

1. INTRODUCTION

Cryptography is the process to convert data from readable form to unreadable form in order to achieve the security requirements. Cryptography or encryption is also providing authentication to user as well as protecting the data. Usually, the original data is called plaintext, and encrypted data is called ciphertext. So the result of convert plaintext to cipher text is called encryption, as well as the result of convert ciphertext to plaintext is called decryption [1] [2]. The cryptography could be classified into two groups which are symmetric and asymmetric encryption. The cryptography is so important in cloud computing because the user must transfer his particular data through the internet to be stored in the cloud [3]. So, without encrypt the data will be easily discovered by the attackers, also in the cloud storage the data must be applied to strong encryption to be protected against attackers [2].

2. CRYPTOGRAPIC GOALS

There are four goals which are almost detected and prevented the attackers to altering, tampering, stealing, etc. the particular data [4]. These goals are:

2.1 Confidentiality

It is the process to ensure that only the authorized person must have an access to data. There are many techniques to provide a confidentiality such as physical protection and encryption algorithms to produce unclear shape for data [4] [5].

2.2 Data integrity

It is the process to ensure the data will sent completely without any modification on it. The modification of data might be substitution, deletion and insertion [4] [6].

2.3 Authentication

It is the process which must help the recipient to identify the received data has come from the real sender only [7][8].

2.4 Non-repudiation

It is the process to ensure both sender and recipient must not refuse the transmission, this mean the sender cannot deny sending the data, as well as the recipient cannot deny to receive the data [8] [9].

3. MECHANISIMS OF CRYPTOGRAPHY

The above four cryptography goals is considered in cryptography mechanisms in order to prevent, detect or recover the unauthorized attackers. The mechanisms of cryptography is classified into two mechanisms [2]:

- Pervasive security: that type of mechanisms which aren’t certain to any specific protocol layer or security service of OSI, such as event detection, security label, etc.
- Specific security: that type of mechanisms which can be included into efficient layer of protocol as a way to supply some security service of OSI, such as digital signature, decipherment, etc.

3.1 Processing Approaches of Plaintext

The encryption of plain text can be done in one of two ways. First way is stream cipher and the second way is block cipher [2][10]. In stream cipher each and every bit in plaintext will combine with pseudorandom key as a way to encrypt the plaintext bit by bit. In block cipher many bits in plaintext will combine together to be processed with single key in order to produce same size of block as a ciphertext. For instance, a block of 128-bits block size of plaintext will be put into encryption algorithm and correspondingly 128-bits block size of ciphertext will be outputted. Block cipher utilizes many operation modes to support data with authenticity or confidentiality. Several operation ways have already been defined examples of these are Counter mode, Output Feedback (OFB), Cipher Feedback (CFB), Cipher Block Chaining (CBC) and Electronic Codebook (ECB) [2] [11].

3.2 Key Distribution

In symmetric encryption the same key which used to encrypt the data must be in recipient side to be able to decrypt same data [12]. Hence, the big issue here is how to handover the key to recipient. There are four methods to deliver the key to recipient, as following [2]:

- Select the key by sender and then delivered physically to recipient.

- Third party must select the key and delivered physically to both sender and recipient. This third party must be pre-trusted by two parties.
- If key used by both sender and recipient recently, so one of them can used same key to encrypt the new key to be sent to other.
- If both of sender and recipient have already encrypted and secure channel connected to a third party, then the third party will be able to handover the key to sender and recipient through same channel.

3.3 Cryptanalysis

As we understood the cryptography is the method to encrypt the plaintext to ciphertext. In the other hand the cryptanalysis is the method which used by attackers to break and analysis the ciphertext to plaintext without knowing the key [13]. Thus, the job of attackers will fall into two purpose. First they got the ciphertext and they want to obtain the key in order to get the plaintext. Second they got the ciphertext and they want to obtain the plaintext without the need of encryption key [14]. So the classical cryptanalysis required a combination of pattern finding, mathematical tools application and analytical reasoning. The attacks of Cryptographic can be grouped into two types, which are active attack and passive attack [15]. It shown in brief as below [2][16][17]:

3.3.1 Active attack

it is the type of attack which attacker here is trying to change the content of data such as altering the contents. So the attackers will alter the original message and resend it to recipient to pretend as it sent from the particular sender.

3.3.2 Passive attack

it is the type of attack which attacker here only read the exact information of message without any alteration on it.

So many other attacks are exist rather than above mentioned, which are trying to break the algorithm of cryptography such as linear cryptanalysis, brute force attack, etc.

4. CLASSIFICATIONS OF CRYPTOGRAPHY

Cryptography systems are fall into three groups which are: symmetric cryptography, asymmetric cryptography and hash functions. Briefly will explained as below [2][18][19]:

1. Symmetric cryptography: it is the technique for convert plaintext into ciphertext using a same key for both sides (sender/recipient). Symmetric cryptography algorithms are AES, DES, Blowfish, RC5, etc.
2. Asymmetric cryptography: which also known as public key cryptography, two keys are used. To encrypt the data by sender, it will encrypt using the public key of recipient which known for any user in network, for decrypt the data the private key of recipient which known only for recipient itself will be used to convert ciphertext to original plaintext. Symmetric cryptography algorithms are RSA, Diffie-Hellman, etc. most of these techniques are using a block cipher to encrypt and decrypt the files.
3. Hash function: it perform transformation by using mathematical to encrypt data irreversibly. Hash function are SHA-1, MD5, etc. The hash function does not have keys as the ciphertext cannot transform to plaintext. The Fig 2.1 shows many different types of cryptographic techniques.

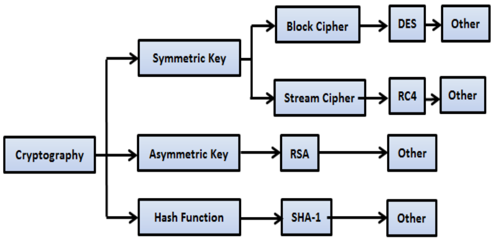

Fig 2.1: Different Types of Cryptographic Techniques. [2]

5. SYMMETRIC KEY CRYPTOGRAPHY

As we mentioned above the symmetric encryption algorithms are using same single key to encrypt and decrypt the data. There are many algorithms of this type such as Blowfish, DES, AES and so on. Each algorithm uses a different method to encrypt and decrypt the data, also each of them will encrypt and decrypt a fixed size of data as a block and fixed size of key. Such type of algorithms will allow only English alphabets, special symbols and numerical values to be entered as a plaintext[2]. Therefore the output (ciphertext) will produced as a document in form of special characters or alphabets or numbers or combining all of them. We can list the components of symmetric encryption as below [2][20]:

1. Plaintext: It is the original data which sender willing to send to specific recipient. These data will be input to the encryption algorithm.
2. Encryption algorithm: It is a set of processes which will execute into plaintext by the help of secret key to produce the ciphertext.
3. Secret key: it is value which used to combine to plaintext in order to transform it to ciphertext, this value will be independent of plaintext.
4. Ciphertext: it is the output of the original plaintext which put to encryption algorithm. it will be extremely different of plaintext.
5. Decryption algorithm: is a set of processes which will be execute to ciphertext by the help of secret key to produce original plaintext.

This paper is giving an idea for the most popular symmetric algorithms. The techniques of cryptographic encryption can be divided into two techniques which are classical cryptographic and modern cryptographic according to the periods that are generally used/developed.

- Classical cryptographic: created in initial days, however some of them are still used these days to providing a proper confidentiality to the data [21].
- Modern cryptographic: created recently, it is purpose was to provide many goals such as authentication, confidentiality, etc.to the data [22].

The algorithms of modern cryptographic is more complex than the algorithms of classical cryptographic to be able to provide a high level of security. Some algorithms of modern cryptographic designed to repeats exactly same procedure for a lot of rounds such as feistel network, etc. there are encryption algorithms which work along with two above techniques, such as hill cipher, one time pad, play fair cipher, etc. the table 1 and 2 which are below is explains most popular algorithms of symmetric encryption, key size, Uniqueness in regards to the technique and Vulnerable to attack.

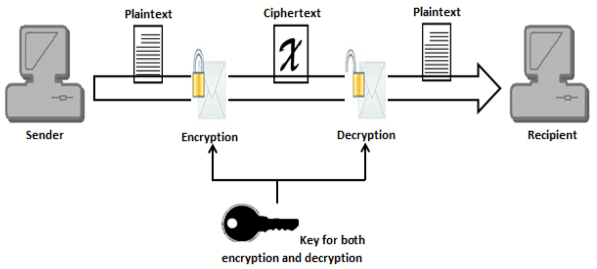

Fig 2.2: Explanation of whole process of symmetric encryption

Table 1. Classical cryptographic algorithms [2] [21] [23][24][25]

S. No.	**Algorithm name**	**Key size**	**Uniqueness in regards to the technique**	**Vulnerable to attack**
1	Caesar cipher	25	Simple alphabet substitution	Brute force Attack
2	Playfair	25	Use two letters and Then substitute them with matrix (5x5) designed with remaining alphabets and key	Frequency Analysis, Brute force Attack
3	Hill Cipher	25	Made from Linear algebra, Convert the plaintext to matrix based on the value of ASCII	Known plaintext attack
4	Vigenere Cipher	25	Organize the letters in shape of 26*26 matrix and achieve substitution with two letters	Kasiski Examination, Frequency Analysis
5	Vernam cipher	25	XOR operation between the bits of plaintext and key.	Known Plaintext attack
6	One time Pad	Exactly same as the size of plaintext	Just like the vigenere cipher but the size of key should be equal to the size of plaintext.	cipher text and Key chosen
7	Rail Fence	-	The plaintext	Chosen

Table 2. Classical cryptographic algorithms [2] [22] [23] [24][26]

S. No.	**Algorithm Name**	**Key size**	**Uniqueness in regards to the technique**	**Vulnerable to attack**
1	Camellia	128, 192, or 256 bits	Nested Feistel Network, number of rounds is 16	algebraic attack
2	Serpent	128, 192 or 256 bits	Open source Algorithm, number of rounds is 32	Rectangle algebraic attack and Linear cryptanalysis
3	Rijndael	128, 192 or 256 bits	Number of rounds is 10,12 or 14 (it depend on the size of key), The maximum size of input file is (2,097,152) bytes	Algebraic attack, Related Key Attack
4	Skipjack	80 bits	Lopsided Feistel Network Structure, 32 rounds	Slide attack
5	AES	128, 192, 256 bits	Number of rounds is 10, 12 or 14, Substitution permutation network	Side channel attack, Known plaintext
6	RC-6	128, 192, 256 bits	Number of rounds is 20, Feistel network	chosen cipher text, Known plaintext
7	SEED	128 bits	Number of	Known

			was created downwards on successive "rails" of some imaginary fence, after that will move up once we arrive at bottom.	Plaintext, Known cipher text
8	Root cipher	-	Just like the Rail fence but rearranging the cipher text as spiral inwards, clockwise, getting started from top right	Chosen Plaintext, Known cipher text
9	Columnar Transposition		Write the plaintext in fixed length of rows, and read them column by column. These columns are chosen in scrambled order.	chosen cipher text, Known plaintext
10	Double Transposition		A columnar transposition executed twice. Different keys or Same key used.	chosen cipher text, Known plaintext
11	Myszkowski Transposition		Have the need for keyword with repeated letters which are identically numbered .	chosen cipher text, Known plaintext
12	Disrupted Transposition		It use the grid for putting the plaintext. It also break-up the regular pattern.	Known Plaintext, Frequency Distribution
13	Grills		It using masks which is physical with cut-outs, or grilles instead of mathematical algorithm	Known Plaintext

			rounds id 16, Nested Feistel Network	plaintext, Chosen plaintext
8	Twofish	128, 256 bits	Feistel Structure. Number of rounds is 16, Free to use	Truncated differential Cryptanalysis
9	CAST-256	128, 160, 192, 224, 256 bits	Feistel Network Structure, number of rounds is 48.	cipher text and known plain text
10	XTEA	128 bits	Variable number of rounds. Nested Feistel Network	chosen plaintexts, Related key differential attack
11	RC-2	8-128 bits (64 bits)	Number of round is 18, Source heavy Feistel Network Structure	Chosen plaintext, Related key attack
12	CAST-128	40 to 128 bits	Feistel Network Structure, Number of round is 12 or 16.	Known plain text and Chosen cipher text
13	RC-5	0 to 2040 bits (suggested 128bits)	It is feistel- just like network, 1 to 255 (advised 12)	Differential attack
14	TEA	128 bits	Feistel Network Structure, The number of rounds are variable	Chosen plaintext, Related key attack
15	Blowfish	32-448 bits	key independent S-box, number of round is 16.	Weak key, Second order differential attack

			Free to use, Feistel Structure.	
16	IDEA	128 bits	Feistel Network Structure, 8.5 rounds	Weak keys
17	TDES	112 or 168 Bits	Three different keys are used, Feistel Network Structure, number of round is 48.	chosen plaintext, Known plaintext, Theoretically possible
18	DES	56 bits	The number of rounds is 16, Left rotating shift, it is Feistel Structure, Substitution a 32-bit Swap	Bruteforce Attack, Linear and Differential Cryptanalysis

6. ADVANTAGE AND DISADVANTAGE OF SYMMETRIC-KEY CRYPTOGRAPHY

There are many advantage of symmetric-key cryptography as well as disadvantages [27][28]:

6.1 Advantages

1. The ciphers of symmetric-key could be design to obtain high data throughput rates. Some implementations of hardware are able to encrypt hundreds of megabytes each second, while the implementations of software may obtain megabytes per second as a throughput rates.
2. In symmetric-key ciphers, keys are comparatively short.
3. The ciphers of symmetric-key can easily be utilized as primitives to build different mechanisms of cryptographic including computationally efficient digital signature schemes, hash functions and pseudorandom number generators (PNG), to name quite a few.
4. The ciphers of symmetric-key can be compiled to give a result of stronger ciphers. uncomplicated transformations which are very simple to be analyzed, but on their weak, could be used to build a strong products of ciphers.
5. The encryption of symmetric-key is seemed to have a huge background, although it need to be recognized that, notwithstanding of inventing the rotor machines previously, a lot of information in this region has been obtained after invention of digital computer, especially the Data Encryption Standard design in the beginning of 1970s.

6.2 Disadvantages

1. In a communication between two-party, the key must keep secret in both ends.
2. There are many pairs of key in large network, these keys must be properly managed. Consequently, the management of the effective key needs the utilization of an unconditionally trusted TTP.
3. To do proper cryptographic, it needs to change the key frequently, and probably for each individual communication session.
4. The mechanisms of Digital signature are developing from the symmetric-key encryption, usually require either the TTP use or large keys size for the purpose of public verification function.

7. CONCLUSION

Many algorithms has been developed to satisfy the security goals which are integrity, confidentiality, non-reputation and authentication. These encryption algorithms can easily be chosen according to the data type which actually being communicated and the channel type which used for communicate the data. Our purpose of this paper is to explain the basic knowledge about the algorithms of encryption and compare the classical cryptographic algorithms with modern cryptographic algorithms based on a number of parameters such as key size, Uniqueness in regards to the technique and Vulnerable to attack.

8. REFERENCES

[1] Stallings, William. Network security essentials: applications and standards. Pearson Education India, 2007.

[2] K. Saranya, R. Mohanapriya, and J. Udhayan, “A Review on Symmetric Key Encryption Techniques in Cryptography,” Int. J. Sci. Eng. Technol., vol. 3, no. 3, pp. 539–544, 2014.

[3] Kahate, Atul. Cryptography and network security. Tata McGraw-Hill Education, 2013.

[4] B. Schneier, “Applied Cryptography,” Electr. Eng., vol. 1, no. [32, pp. 429–455, 1996.

[5] Gulzar, Nikki, et al. "Surveillance Privacy Protection." Intelligent Multimedia Surveillance. Springer Berlin Heidelberg, 2013. 83-105.

[6] Wang, Cong, et al. "Toward secure and dependable storage services in cloud computing." Services Computing, IEEE Transactions on 5.2 (2012): 220-232.

[7] Zager, Robert P., et al. "Rapid identification of message authentication." U.S. Patent Application No. 14/556,332.

[8] M. Agrawal and P. Mishra, “A comparative survey on symmetric key encryption techniques,” Intern. J. Comput. Sci. Eng., vol. 4, no. 5, pp. 877–882, 2012.

[9] Kahate, Atul. Cryptography and network security. Tata McGraw-Hill Education, 2013.

[10] Beaulieu, Ray, et al. "The SIMON and SPECK lightweight block ciphers."Proceedings of the 52nd Annual Design Automation Conference. ACM, 2015.

[11] Komninos, Nikos. "MORPHEUS: AWORD-ORIENTED STREAM CIPHER."International Journal of Computer Research 19.2/3 (2012): 220.

[12] Cao, Ning, et al. "Privacy-preserving multi-keyword ranked search over encrypted cloud data." Parallel and Distributed Systems, IEEE Transactions on 25.1 (2014): 222-233.

[13] Stallings, William. Cryptography and Network Security, 4/E. Pearson Education India, 2006.

[14] Schneier, Bruce. Applied cryptography: protocols, algorithms, and source code in C. john wiley & sons, 2007.

[15] Conti, Greg. Security data visualization: graphical techniques for network analysis. No Starch Press, 2007.

[16] Kahate, Atul. Cryptography and network security. Tata McGraw-Hill Education, 2013.

[17] Jesudoss, A., and N. Subramaniam. "A Survey on Authentication Attacks and Countermeasures in a Distributed Environment." IJCSE, vol 5.2 (2014).

[18] Daemen, Joan, and Vincent Rijmen. The design of Rijndael: AES-the advanced encryption standard. Springer Science & Business Media, 2013.

[19] Kahate, Atul. Cryptography and network security. Tata McGraw-Hill Education, 2013.

[20] Bellare, Mihir, Kenneth G. Paterson, and Phillip Rogaway. "Security of symmetric encryption against mass surveillance." Advances in Cryptology–CRYPTO 2014. Springer Berlin Heidelberg, 2014. 1-19.

[21] Raychev, Nikolay. "Classical cryptography in quantum context."Proceedings of the IEEE 10 (2012): 2015.

[22] Rebeiro, Chester, Debdeep Mukhopadhyay, and Sarani Bhattacharya. "Modern cryptography." Timing Channels in Cryptography. Springer International Publishing, 2015. 13-35.

[23] Saranya, K., R. Mohanapriya, and J. Udhayan. "A Review on Symmetric Key Encryption Techniques in Cryptography." International Journal of Science, Engineering and Technology Research 3.3 (2014): 539-544.

[24] Huang, Yitong. Comparing the Efficiency of Hybrid and Public Key Encryption Schemes. Diss. 2015.

[25] Salomaa, Arto. Public-key cryptography. Springer Science & Business Media, 2013.

[26] Kong, Jia Hao, Li-Minn Ang, and Kah Phooi Seng. "A comprehensive survey of modern symmetric cryptographic solutions for resource constrained environments." Journal of Network and Computer Applications 49 (2015): 15-50.

[27] Agrawal, Monika, and Pradeep Mishra. "A comparative survey on symmetric key encryption techniques." International Journal on Computer Science and Engineering 4.5 (2012): 877.

[28] Iqbal, Md Sarfaraz, Shivendra Singh, and Arunima Jaiswal. "Symmetric Key Cryptography: Technological Developments in the Field." International Journal of Computer Applications 117.15 (2015).