A Review on Symmetric Key Encryption Techniques in Cryptography

SARANYA K
PG Scholar
Dept of CSE
PPG Institute of Technology
Coimbatore-35

MOHANAPRIYA R
PG Scholar
Dept of CSE
PPG Institute of Technology
Coimbatore-35

UDHAYAN J
Assistant Professor
Dept of CSE
PPG Institute of Technology
Coimbatore-35

***ABSTRACT*--- In today's digital communication era sharing of information is increasing significantly. The information being transmitted is vulnerable to various passive and active attacks. Therefore, the information security is one of the most challenging aspects of communication. Cryptography plays an integral role in secure communication and it provides an excellent solution to offer the necessary protection against the data intruders. Over a significant time, data encryption techniques took a massive leap from simple methods to complicated mathematical calculations in order to achieve secure communication. However still with all its complexity cryptographic algorithms are prone to one are many attacks. Therefore this paper presents a detailed study on various symmetric key encryption techniques, its comparison and the attacks to which they are vulnerable to.**

INDEX TERMS--- Cryptography, Symmetric key Cryptography, Cryptanalysis.

1. INTRODUCTION

Cryptography is the art of achieving security by encoding messages to make them non-readable [5]. Cryptography not only protects the information but also provides authentication to the user. Here the original information and encrypted information are referred as plaintext and cipher text respectively. The transformation of plaintext into unintelligible data known as cipher text is the process of encryption. Decryption is the reverse process of encryption i.e. conversion of cipher text into plain text. During communication, the sender performs the encryption with the help of a shared secret key and the receiver performs the decryption. Cryptographic algorithms are broadly classified as Symmetric key cryptography and Asymmetric key cryptography. This section elucidate about services and mechanisms of cryptography, processing approaches of plaintext, key distribution and cryptanalysis. The section 2 presents classifications of cryptography and symmetric key cryptography and various symmetric key encryption techniques are presented in section 3 and section 4 respectively. Finally this paper is concluded in section 5.

1.1. Services and Mechanisms of Cryptography

Cryptography provides four types of services such as confidentiality, integrity, authentication, non-repudiation [8]. A service that enhances the security of the data processing systems and the information transfers of an organization. Confidentiality is production of data from unauthorized disclosure. Integrity provides assurance that the information received are exactly as sent by an authorized entity i.e., information contain no modification, deletion, etc. Authentication ensures that the identity of the sender and receiver of the information. It provides assurance that the communicating entity is the one that it claims to be. Non-repudiation refers to the ability to ensure that the sender or receiver cannot deny the authenticity of their signature on the sending information that they originated.

Cryptography having security mechanism that is designed to detect, prevent or recover from a security attacks. Security mechanism of cryptography is divided into two types such as specific security mechanisms and pervasive security mechanisms. Specific security mechanism may be incorporated into the appropriate protocol layer in order to provide some of the OSI security services for example encipherment, digital signature, etc. Pervasive security mechanisms those are not specific to any particular OSI security service or protocol layer for example security label, event detection, etc.

1.2 Processing Approaches of Plaintext

The plaintexts are processed in two ways; one is the stream cipher and the other is the block cipher [9]. A stream cipher is a symmetric key cipher where plaintext digits are combined with a pseudorandom cipher key stream. In a stream cipher each plaintext digit is encrypted one at a time (encrypt the information by individual bits) with the corresponding digit of the key stream, to give a digit of the cipher text stream. A block cipher is another symmetric key cipher operating on fixed-length groups of bits, called blocks, with an unvarying transformation [16]. For example block cipher encryption algorithm take a 128-bit block of plaintext as input, and output a corresponding 128-bit block of cipher text.

Block ciphers uses modes of operation to provide an information services such as confidentiality or authenticity. Many modes of operation have been defined some of these are Electronic Codebook (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), and Counter mode. A mode of operation describes how to repeatedly apply a cipher's single-block

ISSN: 2278 – 7798

operation to securely transform amounts of data larger than a block.

1.3 Key Distribution

The major problem in symmetric key cryptography is that of the key distribution because the key must be shared secretly [6]. Keys can be distributed by any one of the following ways 1. Sender can select the key and physically deliver it to receiver, 2. A trusted third party can select the key and physically deliver it to the sender and the receiver, 3. If sender and receiver have previously and recently used a key, one party can transmit the new key to the other, encrypted using the old key, 4. If sender and receiver each has an encrypted connection to a third party, then the third party can deliver a key on the encrypted links to sender and receiver.

1.4 Cryptanalysis

While cryptography is the science of securing data, cryptanalysis is the science of analyzing and breaking the secure communication [3]. A cryptanalytic attack can have two possible goals. The cryptanalyst might have cipher text and want to discover the plaintext, or might have cipher text and want to discover the encryption key that was used to encrypt it. Classical cryptanalysis involves an interesting combination of analytical reasoning, application of mathematical tools, pattern finding. Cryptanalysts are also called attackers. Cryptographic attacks are mainly classified as two types, namely passive attack and active attack. Goal of Passive attack is just read the information it does not change the content of the message, for example of message content it only read the content of message without permission. Where as in active attack, not only read the information and also modifying the content of the message. For example replay attack accesses the message that send to the receiver and it sent its own message content to the receiver as like sender. Some other attacks are available to break the cryptographic algorithm such as known plaintext, cipher text only, brute force attack, linear cryptanalysis, etc.

2. CLASSIFICATIONS OF CRYPTOGRAPHY

Cryptography systems can be classified into three types as symmetric key cryptography, asymmetric key cryptography and hash functions. A symmetric key cryptography uses same secret key by sender and receiver for encryption and decryption respectively for example DES, etc [5]. In these techniques the plaintext and key are processed as stream cipher or block cipher. Asymmetric or public key cryptography uses public key by sender for encryption which is known to all and private key which known by the receiver for decryption for example RSA, etc. Mostly this kind of techniques uses block ciphers for processing plaintext with key. The hash function uses mathematical transformation to irreversibly encrypt information for example MD5, etc. It has no keys since the plaintext is not recoverable from the cipher text. Fig 2.1 illustrates types of cryptographic techniques.

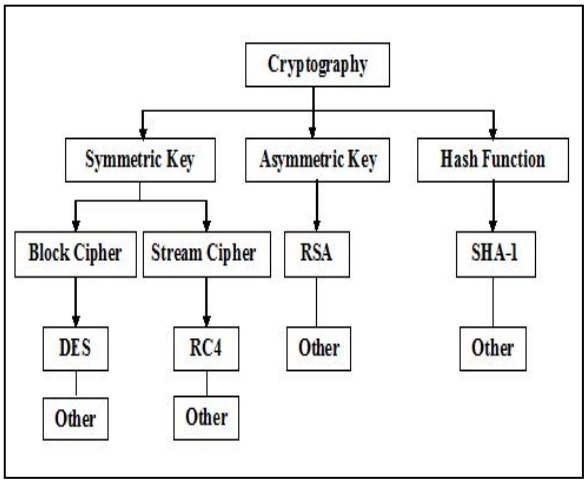

Fig 2.1 Classifications of cryptography

3. SYMMETRIC KEY CRYPTOGRAPHY

In symmetric key cryptographic algorithms single key is used for both encryption and decryption process [5]. Fig 3.1 illustrate that the general procedure for symmetric key cryptographic algorithms. Many symmetric encryption algorithms like DES, AES, Blowfish, RC5, IDEA etc. are available to protect the information. Each algorithm uses different block size, key size and processing method. These algorithms only accept English alphabets, numerical values and special symbols as plaintext. The cipher text will be a document which is in the form of alphabets or special characters or numbers or combination of all. Symmetric key encryption scheme has five components namely plaintext, encryption algorithm, secret key, cipher text, decryption algorithm. Plaintext is an original intelligible data is fed into the algorithm as input. Encryption algorithm performs various operations on plaintext with the help of secret key. Secret key is a value independent of the plaintext which gives as input to the encryption algorithm. Cipher text is scrambled message produced as output. Decryption algorithm takes cipher text and secret key as input and produce plaintext as output by performing encryption algorithm in reverse order.

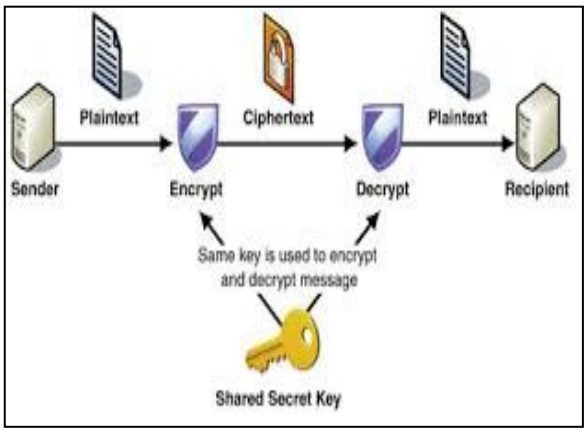

Fig 3.1 Symmetric key encryption process

This paper describes about some of the symmetric encryption techniques which are already available. In

4. VARIOUS SYMMETRIC KEY ENCRYPTION TECHNIQUES

general cryptographic encryption techniques are classified as classical cryptographic techniques and modern cryptographic techniques based on the periods that are developed/used. Classical cryptographic techniques are developed in the earliest days, but still some of the algorithms are used for providing confidentiality to the information. Modern cryptographic techniques are developed in recent years for providing better services like confidentiality, authentication, etc., to the information. In order to increase the degree of security, the modern cryptographic techniques algorithms are incredibly complex than classical cryptographic algorithms. Some of modern cryptographic algorithms are designed in such a way that repeats same procedure for many rounds, for example Feistel network, etc. Besides, symmetric encryption techniques also have encryption algorithms in both of classical and modern cryptographic techniques. For example play fair cipher, one time pad, hill cipher, etc. are comes under classical cryptographic techniques, and DES, AES, etc are modern cryptographic techniques. Here existing symmetric encryption algorithms are compared based on the parameters like block size, size of key, vulnerability to attacks and uniqueness of the technique, which are depicted as tabulation. Table I portrays the comparison of classical encryption techniques that are already exist. Table II illustrates that the comparison of some of the modern encryption techniques that are available.

Table I Classical symmetric encryption algorithms

S.No	Encryption technique name	Year	Developed by	Granularity (stream/ block cipher)	Key Size	Vulnerable to attack	Uniqueness about the technique
1	Caesar Cipher	19th century	Julius Caesar	Block cipher	25 keys	Brute force attack	Simple substitution with alphabet
2	Playfair	1854	Charles Wheatstone	Block cipher	25 keys	Brute force attack, Frequency analysis	Use pair of letters and substitute with 5×5 matrix designed with key and remaining alphabets
3	Hill Cipher	1929	Lester S. Hill	Block cipher	25 keys	Known plaintext attack	Based on Linear algebra, Convert plaintext into matrix based on ASCII value
4	Vigenere Cipher	1553	Giovan Battista Bellaso	Block cipher	25 keys	Frequency analysis, Kasiski examination	Arrange the letters in 26*26 matrix and perform substitution with pair of letters
5	Vernam cipher	1917	Gilbert Vernam	Stream cipher	25 keys	Known plaintext	XOR operation between plaintext bits and key bits
6	One time pad	1882	Frank Miller	Stream cipher	Equal To plain text size	Key and cipher text chosen	Same as vigenere cipher but here key size must be equal to plaintext size
7	Rail Fence	-	Anonymous	-	-	Known cipher text, Chosen plaintext	Plaintext is written downwards on successive "rails" of an imaginary fence, then moving up when we get to the bottom.
8	Root cipher	-	Anonymous	-	-	Known cipher text, Chosen plaintext.	Same as Rail fence but re arranging cipher text as spiral inwards, clockwise, starting from

							the top right.
9	Columnar transposition	-	Anonymous	-	-	Known plaintext, chosen cipher text.	The plaintext is written out in rows of a fixed length, and then read out again column by column, and the columns are chosen in some scrambled order.
10	Double transposition	-	Anonymous	-	-	Known plaintext, chosen cipher text.	A columnar transposition applied twice. Same key or different key used.
11	Myszkowski transposition	1902	Myszkowski	-	-	Known plaintext, chosen cipher text.	Require keyword with recurrent letters which are numbered identically.
12	Disrupted transposition	-	Anonymous	-	-	Frequency distribution, Known plaintext	Use grid for placing the plaintext. It breakup regular pattern.
13	Grills	-	Anonymous	-	-	Known plaintext	Uses grilles, or physical masks with cut-outs, rather than mathematical algorithm

Table II Modern symmetric encryption algorithms

S.No	Encryption technique name	Year	Developed by	Granularity (Stream/ Block Cipher)	Key size	Vulnerable to attack	Uniqueness about the technique
1	Camellia	2000	Mitsubishi, NTT	Block cipher (128 bits)	128, 192, or 256 bits	algebraic attack	16 rounds 8*8 S-boxes. Nested Feistel Network
2	Serpent	1998	Ross Anderson, Lars Knudsen, Eli Biham	Block cipher (128 bits)	128, 192 or 256 bits	Linear cryptanalysis and Rectangle algebraic attack	32 rounds, Open source algorithm
3	Rijndael	1998	Vincent Rijmen, Joan Daemen	Block cipher (128 bits)	128, 192 or 256 bits	Related Key Attack, Algebraic attack	10,12,14 rounds (depending on the key size) maximal size of the input file is 2,097,152 bytes
4	Skipjack	1998	National Security Agency (NSA)	Block cipher (64 bits)	80 bits	Slide attack	32 rounds unbalanced Feistel Network Structure

5	AES	1998	Joan Daemen, Vincent Rijmen	Block cipher (128 bits)	128, 192, 256 bits	Known plaintext, Side channel attack	Substitution-permutation network, 10 or 12 or 14 rounds
6	RC-6	1998	Ron Rivest	Block cipher (128 bits)	128, 192, 256 bits	Known plaintext, chosen cipher text	Feistel network, 20 rounds
7	SEED	1998	Korea Information Security Agency	Block cipher (128 bits)	128 bits	Chosen plaintext, Known plaintext	16 rounds 8*8 s-boxes Nested Feistel Network
8	Twofish	1998	Bruce Schneier	Block cipher (128 bits)	128 256 bits	Truncated differential cryptanalysis	16 rounds Feistel Structure. Free to use
9	CAST-256	1998	Carlisle Adams, Stafford Tavares Howard Heys, Michael Wiener	Block cipher (128 bits)	128 160 192 224 256 bits	Known plain text and cipher text	48 rounds Feistel Network Structure
10	XTEA	1997	Roger Needham, David Wheeler	Block cipher (64 bits)	128 bits	Related key differential attack, chosen plaintexts	Variable rounds. Nested Feistel Network
11	RC-2	1996	Ron Rivest	Block cipher (64 bits)	8-128 bits (64 bits)	Related key attack, Chosen plaintext	18 rounds Source heavy Feistel Network Structure
12	CAST-128	1996	Carlisle Adams, Stafford Tavares	Block cipher (64 bits)	40 to 128 bits	Chosen cipher text and Known plain text	12 or 16 rounds Feistel Network Structure
13	RC-5	1994	Ron Rivest	Block cipher (32,64,128 bits)	0 to 2040 bits (suggested 128bits)	Differential attack	Feistel-like network, 1 to 255(suggested 12)
14	TEA	1994	Roger Needham, David Wheeler	Block cipher (64 bits)	128 bits	Related key attack, Chosen plaintext	Variable rounds Feistel Network Structure
15	Blowfish	1993	Bruce Schneier	Block cipher (64 bits)	32-448 bits	Second-order differential attack, Weak key	16 rounds Feistel Structure. Free to use, key independent S-box
16	IDEA	1991	Xuejia Lai, James Massey	Block cipher (64 bits)	128 bits	Weak keys,	8.5 rounds Feistel Network Structure
17	TDES	1978	IBM	Block cipher (64 bits)	112 or 168 bits	Theoretically possible, Known plaintext, chosen plaintext	48 rounds Feistel Network Structure, Three different keys used
18	DES	1977	IBM	Block cipher (64 bits)	56 bits	Differential & Linear Cryptanalysis, Brute-force attack	16 rounds Feistel Structure, Left circular shift, Substitution 32-bit swap

ISSN: 2278 – 7798

5. CONCLUSION

Cryptography plays vital role in explosive growth of digital data storage and communication. It is used to achieve the mains of security goals like confidentiality, integrity, authentication, non-repudiation. In order to achieve these goals, various cryptographic algorithms are developed. In which some of the algorithms are succeed and others failed due to lack of security. The algorithm for encryption can be selected based on the type of data being communicated and type of channel through which data is being communicated. The main purpose of this paper is to disseminate the basic knowledge about the cryptographic algorithms and comparison of available symmetric key encryption techniques based on some parameters like vulnerability to attack, Uniqueness about the technique, etc.

REFERENCES

[1] Manoj Kumar Pandey, et.all., "Survey Paper: Cryptography The art of Hiding Information", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278 – 1323, Volume 2, Issue 12, December 2013.
[2] Irfan Landge et al., "Encryption and Decryption of Data Using Twofish Algorithm", World Journal of Science and Technology, ISSN: 2231-2587, Vol. 2, No. 3, pp. 157-161, 2012.
[3] Anjali Arora et al., "A Survey of Cryptanalytic Attacks on Lightweight Block Ciphers", International Journal of Computer Science and Information Technology & Security, ISSN: 2249-9555, Vol. 2, No. 2, April 2012.
[4] A. Grediaga et al., "Analysis and Implementation Hardware-Software of Rijindael Encryption", IEEE Latin America Transactions, Vol. 8, No. 1, pp. 82-87, March 2010.
[5] Ayushi, "A Symmetric Key Cryptographic Algorithm", International Journal of Computer Applications, ISSN: 0975 – 8887, Vol. 1, No. 15, 2010
[6] Christof Paar, JanPelzl, and Bartpreneel, "Understanding Cryptography: A Text book for student and Practitioners", Springer, 2010.
[7] Tarun Narayan Shankar and G.Sahoo, "Cryptography by Karatsuba Multiplier with ASCII Codes", International journal on computer applications, pp.53-60, 2010.
[8] William Stallings "Cryptography and Network Security: Principles and Practices", PHI Learning Private Limited, Forth Edition, 2009, pp 64 - 86.
[9] Yee Wei Law, Jeroen Doumen, and Pieter Hartel, "Survey and Benchmark of Block Ciphers for Wireless Sensor Networks", ACM Transactions on Sensor Networks, Vol. 2, No. 1, February 2006.
[10] Chris Christensen, "The Hill Cipher", MAT/CSC 483, 2006.
[11] Bruce Schneier et al., "A Twofish Retreat: Related-Key Attacks Against Reduced-Round Twofish", Twofish Technical Report #6, February14, 2000.
[12] Bruce Schneier et al., "New results on The Twofish Encryption Algorithm", February1, 1999.
[13] Daemen J., Rijmen V., "The Rijindael Block Cipher", AES Proposal, Belgica 1999.
[14] C.Adams, "Constructing Symmetric Ciphers Using the CAST Design Procedure", in selected Areas in cryptography, E. Kranakis and P. Van Oorschot (ed.), Kluwer Academic Publishers, pp. 71-104, 1997.
[15] Ross J. Anderson, "Why Cryptosystems Fail", Communications of the ACM, New York, USA, pp. 32-40, 1994.
[16] Bruce Schneier, "A Self-Study Course in Block-Cipher Cryptanalysis".
[17] Carlisle Adams, "The CAST-256 Encryption Algorithm".
[18] Tom Moore, Kenneth Ballentine, "Serpent Cipher Design and Analysis".
[19] Frank Lin, Cryptographic's past, present and future role in society, Dec 2010.
[20] http://citeseerx.ist.psu.edu (Serpent Cipher)

ISSN: 2278 – 7798