Comparative Study of Security Aspects of Various Symmetric Key Encryption Algorithms

Sreeja Rajesh, Dr. Varghese Paul

Bharathier University
Coimbatore, India
Email: m.sreeja79@gmail.com

Department of Information Science, Cochin University(CUSAT)
Kerala, India
Email: vp.itcusat@mail.com

ABSTARCT--- ***Symmetric Key Cryptography also called secret key cryptography is a simpler and faster means of data transfer through an unreliable channel. It requires fewer overheads in terms of speed and energy cost than Public Key cryptosystem. This paper provides an insight into various security aspects of different Symmetric Key Encryption Algorithms.***

Keywords--- Cryptography, Symmetric Key Encryption, Public Key Cryptosystem, Secret Key

1. INTRODUCTION

In the 21st century, where Internet plays a major role in everyone's day to day life, security of information has become a major concern. Due to the advancement in technology, it has become even more challenging to protect the data from the intruders. "Cryptography" derived from Greek word kryptos meaning "hidden", is an art of protecting information by transforming it into an unreadable format. This scrambling of information (plaintext) using a secret key is called encryption and scrambled data is called cipher text. The process of transforming cipher text back into readable form (plain text) is called decryption. The secret key plays an important role in encryption-decryption process. Cryptographic systems can be broadly classified into symmetric-key systems and public-key systems. Symmetric Key Systems uses a single key that both sender and recipient share and Public-key systems that use two keys, a public key known to everyone and a private key that only the receipt of messages uses.

In this paper, security aspects of different symmetric key encryption algorithms are discussed. This paper is structured as follows: Section II shows various approaches to deal with security of symmetric key encryption. Section III discuss various popular encryption algorithms. Section IV discuss about the various attacks on these algorithm. Section V gives comparison of popular encryption algorithm with respect to the algorithm structure, key size, block size, number of rounds used etc. Feistal structure- ex: DES, TEA, Blowfish, Two fish RC, Substitution Permutation network, Use of Logistic map, use of DNA coding, use of 2D geometry etc are some techniques.

2. TECHNIQUES FOR SECURE ENCRYPTION

DNA Coding [1], as proposed in the paper "Bit based Symmetric Encryption Method using DNA sequence" use DNA sequence as a Key and complementary rule pair. Using this method any form of data including image, audio, video or text file can be encrypted. DNA cryptography uses DNA as an information carrier and it is a combination of computer science domain and biological domain. DNA was first identified by Swiss physician Friedrich Mieschеir in 1869 [2]. DNA cryptography first converts the data in the form of DNA sequence. After conversion of data, security is applied by using biological or arithmetic operations like chain reactions, transcription and translation etc. DNA cryptography was introduced by Dr. Leonard M. Adelman of University of South California in 1994 to solve the complex mathematical problem.

Logistic map, a polynomial mapping which exhibits chaotic behavior as proposed in the paper "Symmetric Encryption using Logistic Map [3] uses sensitive to initial condition property. Devaneys definition of chaos [4] indicated that two conditions x0 and x0 ' where x0 ≠ x0 ' no matter how close they are, will turn into very different states quickly through the evolutions of map. Sensitivity to initial conditions property of chaos can be exploited to produce avalanche effect by which makes two nearby keys to produce different cipher text.

Planar geometric computation in 2D[5] coordinates can be considered for encryption. The paper " A New Symmetric Key Encryption Algorithm based on 2-d Geometry"[6] uses the property of circle and circle-centered angle. Shared key is a pair of geometric points (center O of the circle, shared secret point S lying on the perimeter of the circle). Radius of circle is computed as r2 = (sx - cx) 2 + (sx - cy) 2 and C,Sx and r are transmitted as shared secret key. On receiving these values Sy has to be computed. The problem with this approach is that floating point calculation and round off operation limits the size of block to encode. Hence increasing the block size may subject to round off error, also hardware implementation can be tedious and very tricky.

Feistel Structure was proposed by Feistel. According to this structure the plaintext block of length 2w bits and a key k are the inputs to the encryption algorithm. The plaintext is divided into two halves L0 and R0. These two halves of data passes through n rounds of processing and then combine to produce ciphertext. All rounds have same structure. A substitution is performed in each round by applying round function to the right half of the data and then taking XOR of the output of that function and left half of the data. In each round a different subkey is provided. Following substitution, a permutation is performed by interchanging the two halves of data.

Nonce-Based was proposed by Phillip Rogaway in his paper "Nonce-Based Symmetric Encryption"[7]. An important property of Nonce-Based encryption is that, ciphertext produced by an intruder coupled with its nonce value should be considered invalid at the receiver end unless it is a copy of prior ciphertext and its nonce. Strong properties for a nonce-based encryption scheme are Authenticity[8,9], Chosen-ciphertext security, Nonmalleability[10] etc. In this approach the encryption algorithm is made a deterministic function, but one of its argument is an initialization vector which is supplied by the user. Hence user is made responsible in maintaining the state. Many books suggest that, IV in CBC encryption to be a counter or the last block of encrypted ciphertext. But both statements are wrong if one is intending to achieve strong notion of privacy. Author's notion of privacy is "indistinguishability from random bits under an adaptive chosen-plaintext-and-IV attack". This attack allows the adversary to select both plaintexts and also the IVs that will be used to encrypt each of them, subject only to the constraint that no IV is reused. The model captures the possibility that the IVs may be chosen in an unfortunate way by the sender, possibly even influenced by the adversary, when we do not mandate any requirement on an IV beyond its non-reuse. The area of interest is on providing security properties as long as IV is a nonce used at most once within a session.

Boolean Function was proposed by Muna Abdulla Al Shehhi , Joonsang Baek, Chan Yeob Yeun in " The Use of Boolean Functions in Stream Ciphers"[11]. Boolean function properties such as balancedness[12], high nonlinearity[13] and high algebraic degree[12] play an important role in cryptography especially in the design of S-box for block ciphers and in design of pseudo-random generators for stream ciphers of symmetric key encryption schemes. In this paper the authors suggest different ways of constructing appropriate Boolean functions with good cryptographic characteristics needed to design stream ciphers. Some of open problems identified are: 1) When constructing Boolean functions using primitive polynomials, there is no general form of $p(x)$ such that f has good cryptographic property for any odd n. 2)How tight is the nonlinearity bound of resilient Boolean functions? 3)If n is greater than 8 we still do not know the number of bent functions in n variables. A concept called C criterion profile for Boolean function. ("C" stands for chosen cryptographic property.) [14] is applied to tell how strong a given Boolean function is when we fix some of its input coordinates. The idea behind such a method is that fixing the coordinates of a cryptosystem sometimes results in meaningful cryptanalysis.

3. POPULAR ENCRYPTION ALGORITHMS

TEA, Tiny Encryption Algorithm is a block cipher notable for its simplicity of description and implementation, typically a few lines of code. TEA was designed by David Wheeler and Roger Needham of Cambridge Computer Laboratory in 1994. It operates on two 32 bits unsigned number and uses simple key schedule. Magic constant is used in computing the key. Different multiples of magic constant are used to prevent simple attacks based on symmetry of rounds.

Blow Fish, was designed by Bruce Schneier in 1993 as a fast alternative to AES, DES and Triple DES. It is simple and uses addition, XOR aand lookup table with 32 bit operands. It is considered secure as key length is variable from 32 to 448 bits. It is compact as it can be run in less than 5K of memory. It is fast and encrypts data on 32 bit microprocessor with a rate of 26 clock cycles per byte.

RC2 was published as an Internet Draft during 1997. It was designed by Ron Rivest in 1989. A significant feature of RC2 is its flexibility offered to the user in terms of effective keysize.

DES or Data Encryption Standard was developed on early 1970 at IBM based on Feistal Structure. Due to small key size of 56 bits this algorithm has become insecure. In January 1999 distributed.net and Electronic Frontier Foundation collaborated to publicly break a DES key in 22 hours and 15 minutes. NIST, National Institute of Standards and Technology has withdrawn DES as a Standard.

Triple DES is an enhancement to the DES and it is believed to be practically secure, although there are theoritical attacks. Triple DES uses three DES keys K1, K2 and K3 each of 56 bits and encryption algorithm is as follows:

ciphertext = EK3(DK2(EK1(plaintext)))

that is encrypt plaintext with key K1, then decrypt the resultant cipher with key K2, finally encrypt the result with key K3. The reverse procedure is the Decryption algorithm. There are three Keying options: Keying Option 1: All keys are Independent. Keying option 2: K1 and K2 are independent, and K3=K1. Keying option 3: All Keys are identical, K1=K2=K3. Among the three Keying options Key option 1 is the strongest with 168 (3 x 56) independent key bits.

Rijndal, later named as AES Advanced Encryption Standard was developed by two Belgium cryptographers Joan Daemen and Vincent Rijmen. Rijndael is a family of ciphers with different key sizes 128, 192, 256 bits and block size of 128bits. AES is worldwide used as it has been approved as standard by National Institute of Standards and Technology(NIST).

4. CRYPTANALYSIS

Cryptanalysis is a process of decrypting the ciphertext without knowing the key. This activity is done by the intruders. All the cryptographic algorithms are developed keeping in mind that the information should not be available to anyone without the exact secret key. There are various ways by which the cryptanalyst tried and attacked many algorithms. Some of the attacks are:

Relative Key Attack, in which the attacker can observe the operation of the cipher under several different keys whose values are initially unknown, but where some mathematical relationship connecting the keys are known to the attacker.

Brute Force attack, also known as exhaustive key search attack is a trial and error method that the intruder uses to get the plaintext. Key length used determines whether it is feasible for an intruder to use brute-force attack. Currently, it is considered that key length of 128 bits to be safe and one of the measures to determine the strength of encryption algorithm is how long it will take an intruder to mount a successful brute-force attack.

Differential analysis is called first-order differential analysis where one sample in each trace is needed at the point of attack. By using table masking counter measure where masks randomly change this type of attack can be thwarted.

Second-order Differential attack is more difficult where two samples are required. One is sample of the mask and another is sample of masked data. This type of attack is very difficult because the attackers do not know the location of data, hence all the samples need to be considered.

Truncated differential cryptanalysis is a generalization of differential cryptanalysis. It was developed by Lars Knudsen in 1994. Differential cryptanalysis analyses the full difference between two text, whereas the truncated differential cryptanalysis does not consider the full block, instead the differences are only partially determined. The attack makes predictions of only some of the bits.

5. COMPARATIVE TABLE OF ENCRYPTION ALGORITHMS

Comparisons of Symmetric Encryption Algorithm is shown in the Table 1.

Table 1. Comparisonsable captions should be placed above the table

Algorithms	**Features**		
	Key Size(bits)	**Block Size(bits)**	**Rounds**
TEA	128	64	64(32 cycles)
Blow fish	32 to 448 (128 default)	64	16
Two fish	128, 192 ,256	128	16
RC2	8 to 128(64 default)	64	16 Mixing, 2 Mashing
Triple DES	112 or 168	64	48
DES	56	64	16

Details regarding the algorithm structure and their weakness is shown in Table 2.

Table 2. Weaknesses of Popular Symmetric Encryption Algorithms

Algorithms	**Features**		
	Created by	**Cracked?**	**Existing Cracks**
TEA	David J Wheeler & Roger M Needham(1994)	YES	Equivalent key attack, related key attack
Blow fish	Bruce Schneier(1993)	NO	Second Order Differential attack
Two fish	Bruce Schneier(1993)	NO	Truncated differential cryptanalysis
RC2	Ron Rivest(1987)	YES	Related Key attack
Triple DES	IBM(1978)	NO	Theoritically possible
DES	IBM(1975)	YES	Brute Force attack

6. CONCLUSION

This paper will provide an insight into various security features incorporated in various symmetric encryption algorithms. Research scholars can compare the strength and weakness of many algorithms which might help them in their research.

7. REFERENCES

[1] Shipra Jain, Vishal Bhatnagar, "Bit Based Symmetric Encryption Method Using DNA sequence", pp495-498, 2014 IEEE

[2] M.E. Jones, "Albrecht Kossel, A Biographical Sketch", Yale Journal of Medicine, Vol. 26, Issue No. 1, 1953, pp.80-97.

[3] P. Jhansi Rani, S. Durga Bhavani, "Symmetric Encryption using Logistic Map", IEEE 2012.

[4] R. L. Devaney, "An Introduction to chaotic dynamical systems", Addison-Wesley, 1989.

[5] Dus ans Gupta, Planar Geometry(2nd edition).

[6] Mohammad Jabed Morshed .chowdhury, Tapas Pal, "A New Symmetric Key Encryption Algorithm based on 2-d Geometry.

[7] Phillip Rogaway, "Nounce Based Symmetric Encryption", B.Roy and W. Meier(Eds.): FSE 2004, LNCS 3017, pp.348-359, 2004.

[8] P.Rogaway, M.Bellare,J.Black and T.Krovertz. OCB: block-cipher mode of operation for efficient authenticated encryption. Proceedings of the 8th ACM Conference on Computer and Communications Security (CCS '01), ACM Press, pp. 196–205, 2001.

[9] P.Rogaway, Authenticated-encryption with associated-data. *Proceedings of the 9th ACM Conference on Computer and Communications Security* (CCS '02), ACM Press, pp. 98–107, 2002.

[10] D.Dolev, C.Dwork and M. Naor. Non-malleable cryptography. *SIAM J. Computing*, vol. 30, no. 2, pp. 391–437, 2000.

[11] Muna Abdulla Al Shehhi , Joonsang Baek, Chan Yeob Yeun. "The Use of Boolean Functions in Stream Ciphers", IEEE 6th Inter. Conf. Inf. Tech, pp. 29-33, 2011.

[12] C. Carlet. " Constracting balanced functions with optimum algebraic immunity," IEEE Inter. Symp. Inf. Theorey, pp. 451-455, 2007.

[13] L. Burnett, W. Millan, E. Dawson and A. Clark, " Simple methods for generating better Boolean functions with good cryptographic proporties," Australasian Journal of Combinatorics, vol. 29, pp. 231- 247, 2004.

[14] E. Elsheh, A. B. Hamza and A. Youssef, "ON THE NONLINEARITY PROFILE OF CRYPTOGRAPHIC BOOLEAN FUNCTIONS," IEEE Canad. Conf. Elec. Comp. Eng., pp. 1767- 1770, 2008.