Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 12, December 2014, pg.410 – 415

RESEARCH ARTICLE

Symmetric Key Cryptography: Current Trends

Preeti Singh[1], Praveen Shende[2]

[1]M. Tech. Scholar, CSE Department, Chhatrapati Shivaji Institute of Technology, Durg, India

[2]Asst. Professor, CSE Department, Chhatrapati Shivaji Institute of Technology, Durg, India

[1] preetisingh.research@gmail.com; [2] praveenshende@csitdurg.in

Abstract— The present day & age is the time when Information has become the most powerful commodity & communication online or through wireless networks has become an integral part of our lives. The data being transmitted is prone to various passive and active attacks. Thus, information security is in all likelihood the most formidable part of correspondence today. The solution to this problem is the use of cryptography techniques. Cryptography is the art and science of secret writing that changes the message from its typical structure into a garbled structure. The point of this paper is to portray an expansive review of Encryption & Decryption & provide an involved review of the various Symmetric Key Cryptography algorithms.

Keywords— Cryptography, Encryption, Decryption, Survey, Symmetric Key

I. INTRODUCTION

Cryptography is the study of information hiding and retrieval. Cryptography is derived from the Greek words: kryptós, "hidden", and gráphein, "to write" - or "hidden writing". It is the art of protecting the information by transforming it into an unintelligible format in which a message can be hidden from reader and only the intended recipient will be able to convert it into original message. All intruders or unauthorised readers can only see gibberish. Its main goal is to keep the data safe from unauthorized access. It includes the guidelines, algorithms and methodologies to safely and consistently prevent or delay unauthorized access to vital information and helps verify all components in a communication. Individuals who examine and create cryptography are called cryptographers. The investigation of how to evade the utilization of cryptography for unintended beneficiaries is called cryptanalysis, or code-breaking. Cryptography and cryptanalysis are once in a while gathered together under the umbrella term cryptology,

Symmetric Encryption algorithms play a primary role in information security. So this paper has surveyed the most common algorithms and standards available for the encryption of information in the digital form. An encryption algorithm would be useless if it is secure but takes long time in execution. The field of cryptography is becoming very important in today's times as information security is of absolute importance. Contemporarily more and more sensitive data is being stored on computers and transmitted over the Internet. We need to ensure security and safety of information.

II. BASIC TERMS

An easy way to comply with the conference paper formatting requirements is to use this document as a template and simply type your text into it.

A. Plain Text

The original message that someone wishes to another is defined as Plain Text. In cryptography the real message that has to be sent to the other end is given a special name as Plain Text. Suppose Alice wishes to send

© 2014, IJCSMC All Rights Reserved

the message, *"We shall meet behind the monument in the garden."* to Bob. Here *"We shall meet behind the monument in the garden."* is the plain text.

B. Cipher Text

The message that cannot be understood by anyone or meaningless message is what we call as Cipher Text. In Cryptography the original message is transformed into non readable message before the transmission of actual message. For example, *"Jr funyy zrrg oruvaq gur zbahzrag va gur tneqra."* is a Cipher Text produced for *"We shall meet behind the monument in the garden."* after applying the Caesar's Cipher with key = 13.

C. Encryption

A process of converting Plain Text into Cipher Text is called Encryption. Cryptographers use various encryption methods to send confidential messages via an insecure channel. The process of encryption requires two things - an encryption algorithm and a key. An encryption algorithm means the method that has been used in encrypt the data. Encryption happens at the sender's side.

D. Decryption

The reverse process of encryption is called Decryption. It is the process of converting Cipher Text into Plain Text. Cryptographers use the decryption algorithms at the receiver side to obtain the original message from non readable message i.e. Cipher Text. The process of decryption requires two things - a Decryption algorithm and a key. A Decryption algorithm means the method that has been used in Decryption. Generally the encryption and decryption algorithm are identical but reverse.

E. Key

A Key is a string of alpha numeric characters, which is used to encrypt & decrypt the message. The Key is used at the time of encryption that works on the Plain Text and at the time of decryption works on the Cipher Text. The selection of key in Cryptography is vital as the security of encryption algorithm depends directly on it. For example, if Alice uses Hill Cipher & a key [11 10 20 09] to encrypt the Plain Text *"Gold is buried under the bush of Red Roses!"* then Cipher Text produced will be *"ymvnikdshwwdmxvsnrnudsihwntmvfwaqi"*.

F. Encoder

An encoder is the person that wants to send the message & uses encryption to make the message secure.

G. Decoder

A decoder is the person who decrypts the message. This may be the intended recipient of the message or may be an intruder, trying to get access to the secret message.

III. THE SYMMETRIC CIPHER MODEL

Symmetric encryption transforms plaintext into cipher-text using a secret key and an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the cipher-text [1]. A Symmetric encryption scheme has five ingredients... Plaintext, Encryption Algorithm, Secret Key, Cipher-text and Decryption Algorithm. The Secret Key is shared by both, the sender and the receiver which they must have obtained in a secure fashion & should keep the key hidden, lest anyone who finds the key would be able to extract the hidden message. Figure 1, illustrates this process.

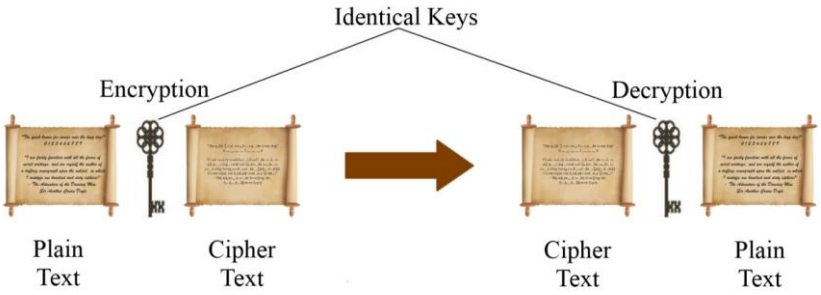

Fig 1: The Symmetric Cipher Model

© 2014, IJCSMC All Rights Reserved

The Symmetric encryption, also referred to as the conventional system, or single-key system, was the only type of encryption in use prior to the development of Public-Key encryption in the 1970s. It remains by far the most widely used of the two types of encryption [1]. It was in use way before the computer era, and can be traced back to the ancient Rome & Egypt. The ciphers which were in use before the advent of the computers are termed as the classical encryption algorithms. They were all very intriguing & worked on texts, but now is the time of bits & bytes. Ergo, many new ciphers were created to help maintain the secrecy of the digital information. The next section of this paper takes a look at the modern symmetric cryptographic algorithms.

IV. OVERVIEW OF SOME COMMON SYMMETRIC CIPHERS

An Symmetric encryption algorithms are extremely effective at transforming a lot of data and computationally less intensive than asymmetric encryption algorithms. There are two sorts of symmetric encryption algorithms: stream ciphers and block ciphers which provide bit-by-bit and block encryption respectively. There are different symmetric key algorithms, for example, DES, TRIPLEDES, AES, RC2, RC4, RC5, RC6, BLOWFISH and TWOFISH. Brief descriptions of the common modern symmetric algorithms are given as follows...

A. *Data Encryption Standard (DES):* DES is the most widely used symmetric cipher. It was designed by IBM based on their Lucifer Cipher. DES is a 64 bit block cipher which means that it encrypts data 64 bits at a time. DES is based on a cipher known as the Feistel block cipher. This was a block cipher developed by the IBM cryptography researcher Horst Feistel in the early 70's. As with most encryption schemes, DES expects two inputs - the plaintext to be encrypted and the secret key. It consists of a number of rounds where each round contains bit-shuffling, non-linear substitutions (S-boxes) and exclusive OR operations. Initially, 56 bits of the key are selected from the initial 64 by permuted choice. The remaining eight bits are either discarded or used as parity check bits. The 56 bits are then divided into two 28-bit halves; each half is thereafter treated separately. In successive rounds, both halves are rotated left by one or two bits and then 48 sub key bits are selected by permuted choice(2),24 bits from the left half and 24 from the right. The key schedule for decryption is similar, the sub keys are in reverse order compared to encryption.

B. *Triple DES:* Triple Data Encryption Algorithm block cipher applies the DES cipher three times to each block of data. The original DES cipher's key size of 56 bits was initially sufficient, but the increase in computational power with time made brute-force attacks feasible. Triple DES provides an easy method of increasing the security of DES to protect against such attacks. It takes three 64-bit keys, making an overall key length of 192 bits. Applying DES three times consecutively using the three different keys it makes the encryption triple strong. Triple DES runs three times slower than DES, but it much more secure. The method for decrypting is the same as the method for encryption, except it is executed backwards.

C. *Advanced Encryption Standard (AES):* The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, who submitted a proposal to NIST during the AES selection process. AES is a block cipher with a block length of 128 bits. AES allows for three different key lengths: 128, 192, or 256 bits. Encryption consists of 10 rounds of processing for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys. Except for the last round in each case, all other rounds are identical. Each round of processing includes one single-byte based substitution step, a row-wise permutation step, a column-wise mixing step, and the addition of the round key. The order in which these four steps are executed is different for encryption and decryption.

D. *RC2:* In cryptography RC2 (also known as ARC2) is a symmetric block-key cipher designed by Ron Rivest in 1987. "RC" stands for "Ron's Code" or "Rivest Cipher". The development of RC2 was sponsored by Lotus under the guidance of NSA. Lotus were seeking a custom cipher that could be exported as part of their Lotus Notes software. Initially, the details of the algorithm were kept secret but source code for RC2 was anonymously posted to the Internet. RC2 is a 64-bit block cipher with a variable size key. Its 18 rounds are arranged as a source-heavy Feistel network, with 16 rounds of one type (MIXING) punctuated by two rounds of another type (MASHING) [5].

E. *RC4:* Another cipher designed by Ron Rivest, RC4 was initially a trade secret, but in the year (1994) that it was created, a description of it was leaked on the Internet and was confirmed to be genuine as it was yielding the same result as the licensed RC4. The name RC4 is trademarked, so RC4 is frequently alluded to as ARCFOUR or ARC4 (meaning alleged RC4) to stay away from trademark issues. RSA Security has

© 2014, IJCSMC All Rights Reserved

never formally released the algorithm; Rivest has, in any case, linked to the English Wikipedia article on RC4 in his own course notes. RC4 has gotten to be a piece of some commonly utilized encryption conventions and guidelines, including WEP and WPA for wireless cards and TLS.

F. *RC5:* In cryptography, RC5 is a symmetric-key block cipher notable for its simplicity. Designed by Ronald Rivest in 1994, RC stands for "Rivest Cipher", or alternatively, "Ron's Code". The Advanced Encryption Standard (AES) candidate RC6 was based on RC5. Unlike many schemes, RC5 has a variable block size (32, 64 or 128 bits), key size (0 to 2040 bits) and number of rounds (0 to 255). The original suggested choices of parameters were a block size of 64 bits, a 128-bit key and 12 rounds. A key feature of RC5 is the use of data-dependent rotations; one of the goals of RC5 was to prompt the study and evaluation of such operations as a cryptographic primitive. RC5 also consists of a number of modular additions and exclusive-OR (XOR)s. The general structure of the algorithm is a Feistel-like network [5].

G. *RC6:* Rivest Cipher 6 (RC6) is a symmetric key block cipher derived from RC5. It was designed by Ron Rivest, Matt Robshaw, Ray Sidney, and Yiqun Lisa Yin to meet the requirements of the Advanced Encryption Standard (AES) competition. The algorithm was one of the five finalists, and also was submitted to the NESSIE and CRYPTREC projects. It is a proprietary algorithm, patented by RSA Security. RC6 is very similar to RC5 in structure, using data-dependent rotations, modular addition, and XOR operations; in fact, RC6 could be viewed as interweaving two parallel RC5 encryption processes, however, RC6 does use an extra multiplication operation not present in RC5 in order to make the rotation dependent on every bit in a word, and not just the least significant few bits [11].

H. *Blowfish:* Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993[2] by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and key can be any length up to 448 bits. It is significantly faster than most encryption algorithms when implemented on 32- bit microprocessors with large data caches. The algorithm consists of two parts: a key expansion part and a data-encryption part. Key expansion converts a key of at most 448 bits into several sub keys arrays totalling 4168 bytes [3].

I. *Twofish:* Twofish is a symmetric key block cipher with a block size of 128 bits and key sizes up to 256 bits. It was one of the five finalists of the AES contest, but was not selected for standardization. Twofish has been developed on the earlier block cipher Blowfish. It was designed by Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, and Niels Ferguson. The Twofish cipher has not been patented and the reference implementation has been placed in the public domain. As a result, the Twofish algorithm is free for anyone to use without any restrictions whatsoever. It is one of a few ciphers included in the OpenPGP standard (RFC 4880). However, Twofish has seen less widespread usage than Blowfish, which has been available longer. Twofish's distinctive features are the use of pre-computed key-dependent S-boxes, and a relatively complex key schedule. One half of an n-bit key is used as the actual encryption key and the other half of the n-bit key is used to modify the encryption algorithm (key-dependent S-boxes) [13].

V. COMPARISON

In this section, various aspects of the above mentioned ciphers are listed in form of a table to provide a clearer understanding of their commonalities & contrasts. The table provides a comparison of nine of the contemporary encryption ciphers by looking at seven of their features.

© 2014, IJCSMC All Rights Reserved

Table 1: Comparison of various Symmetric Ciphers

Algorithm	**Creator**	**Block size**	**Key length**	**Rounds**	**Algorithm**	**Effectiveness**	**Attacks**
DES	IBM (1975)	64 bits	56 bits	16	Fiestel Network	Slow	Brute Force
3DES	IBM (1978)	64 bits	64*3 = 192 bits	48	Fiestel Network	Slow specially in Software	Theoretically Possible
AES	J. Daemen and V. Rijmen (1998)	128, 192, 256 bits	128, 192, 256	9, 11, 13	Substitution Permutation Network	Effective in both Hardware & Software	Side Channel Attacks
RC2	Ron Rivest (1994)	64 bits	8 – 1024 bits	16	Source Heavy Fiestel Network	Efficient in Software	Related Key Network
RC4	Ron Rivest (RSA Security) (1994)	2064 bits, 1684 effective	40 – 2048 bits	256	Fiestel Network	Effective in both Hardware & Software	Fluhrere Mantin & Shamir Attack
RC5	Ron Rivest (1994)	32, 64, 128 bits	0 – 2040 bits (128 suggested)	1 – 255 (12 suggested originally)	Fiestel Network	Slow	Differential Attack
RC6	Ron Rivest etal. (1998)	128 bits	128, 192, 256 bits	20	Fiestel Network	Slow	Brute Force
BLOWFISH	Bruce Schneier (1993)	64 bits	32 – 488 bits (128 default)	16	Fiestel Network	Efficient in Software	Differential Attack , Pseudorandom Permutation
TWOFISH	Bruce Schneier et al. (1998)	128 bits	128, 192, 256 bits	16	Fiestel Network	Efficient in Software	Truncated Differential Cryptanalysis (Partially Broken)

VI. CONCLUSIONS

In this paper various symmetric key encryption algorithms were observed from many angles. Many features were looked at & compared with the other ciphers. Some ciphers are better than others in some aspects but lack behind on others. Each method has its own advantages & shortcomings. To sum up, all the techniques are useful for real-time encryption. Each technique is unique in its own way, which might be suitable for different applications. Everyday new encryption technique is evolving hence fast and secure conventional encryption techniques will always work out with high rate of security. To overcome the problems in Symmetric Ciphers, Public Key Cryptography was developed, but it has its own loopholes. Latest research is going on the topics like DNA Cryptography & Quantum Cryptography. The strongest ciphers of today may become easier to decode with the onset of Quantum Computing. Ergo, there will always be a need for stronger encryption techniques & there is allot of scope for research in the mysterious field of Cryptography.

© 2014, IJCSMC All Rights Reserved

REFERENCES

[1] Stallings W., "Cryptography and Network Security: Principles and Practices", 4'th Ed., Pearson Education 2006, ISBN: 81-7758-774-9
[2] Diffie W., Hellman M.E., New Directions in Cryptography", IEEE Transactions on Information Theory, Vol. IT22 No. 6, November 1976, pp. 644-654
[3] E. Surya, C.Diviya, "A Survey on Symmetric Key Encryption Algorithms", IJCSCN, Vol 2(4), 475-477, ISSN:2249-5789
[4] E. Thambiraja, G. Ramesh, Dr. R. Umarani, "A Survey on Various Most Common Encryption Techniques", IJARCSSE, Volume 2, Issue 7, July 2012 ISSN: 2277 128X
[5] T. Gunasundari, Dr. K. Elangovan, "A Comparative Survey on Symmetric Key Encryption Algorithms", IJCSMA, Vol.2 Issue. 2, February- 2014, pg. 78-83 ISSN: 2321-8363
[6] Thakur J., Kumar N., "DES, AES and Blowfish: Symmetric Key Cryptography Algorithms Simulation Based Performance Analysis", IJETAE, ISSN 2250-2459, Volume 1, Issue 2, December 2011, pp. 6-12
[7] John Justin M, Manimurugan S, "A Survey on Various Encryption Techniques", IJSCE, Volume-2, Issue-1, March 2012, pp. 429-432, ISSN: 2231-2307
[8] Kapsepatil A., Prof. Shah P., "A Literature Survey on Symmetric Encryption Algorithms for Digital data", IJAIR, 2012 pp. 306-308, ISSN: 2278-7844
[9] Patil A, Goudar R, "A Comparative Survey Of Symmetric Encryption Techniques For Wireless Devices", IJSTR, Vol 2, Issue 8, Aug 2013, pp. 61-65, ISSN 2277-8616
[10] Cryptography http://en.wikipedia.org/wiki/Cryptography
[11] RC6: http://en.wikipedia.org/wiki/RC6
[12] Blowfish: http://en.wikipedia.org/wiki/Blowfish_(cipher)
[13] Twofish: http://en.wikipedia.org/wiki/Twofish

© 2014, IJCSMC All Rights Reserved