National Conference on "Recent Trends in Mathematical Modeling, Simulation Methods, Computations, and Physical Sciences"
(MMSCP-2019), Organised by Hislop College, Nagpur, Maharashtra, India
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2019 IJSRCSEIT | Volume 4 | Issue 4 | ISSN : 2456-3307

Comparative Study of Symmetric Key Cryptographic Algorithms CAST, IDEA, RC, Camellia and SAFER

Dr. Harshala B. Pethe[1], Dr. Manish T. Wanjari[2]
[1]Dr. Ambedkar College, Deekshabhoomi Nagpur, Maharashtra, India
[2]SSESA's, Science College, Congress Nagar, Nagpur , Maharashtra, India

ABSTRACT

Information security plays very important role in storing and transmitting the data through unsecured channel. In the network security, cryptography plays vital role to maintain the CIA triad that is Confidentiality, Integrity, Authentication and non-repudiation of information. Therefore the security of information is much important in data storage and transmission process. Cryptography also ensures that the message should be sent without any change and only the intended authorized person can be able to read the message. There are various cryptographic techniques developed for achieving secure communication. Using cryptography, the data is encoded before sending it and decoded after receiving, Cryptographic algorithms are broadly divided into two types, symmetric key and asymmetric key cryptographic algorithms. This paper deals with the comparative study of various symmetric key cryptographic algorithms CAST, IDEA, RC, Camellia and SAFER.

Keywords : Symmetric key cryptography, CAST, IDEA, RC, Camellia and SAFER

I. INTRODUCTION

Cryptography deals with the securing of digital data. It refers to the design of mechanisms based on mathematical algorithms that provide fundamental information security services. It is an establishment of a large toolkit containing different techniques in security applications.

Depending on the key used, cryptographic algorithms are divided into major two types:

1) Symmetric key or private key cryptography.
2) Asymmetric key or public key cryptography.

The private cryptography is an encryption process where key used to encrypt the message is the same as the key decrypting the message [1]. Private key cryptography is fast and efficient, making it ideal for large data transmissions. Private key cryptography is more effective when used with public key cryptography because it is much faster.

II. SYMMETRIC KEY OR PRIVATE KEY CRYPTOGRAPHY

Some symmetric key cryptographic algorithms are explained below:

2.1 Carlisle Adams and Stafford Tavares (CAST)

CAST was designed in Canada by Carlisle Adams and Stafford Tavares. They claim that the name refers to their design procedure and should conjure up images

of randomness, but note the authors' initials. The example CAST algorithm uses a 64-bit block size and a 64- bit key.

The algorithm uses six S-boxes with an 8-bit input and a 32-bit output. Construction of these S-boxes is implementation-dependent and complicated CAST-128 is a DES–like substitution-permutation crypto algorithm, employing a 128-bit key operating on a 64-bit block. CAST-256 is an extension of CAST-128, using a 128-bit block size and a variable length (128, 160, 192, 224, or 256 bit) key. CAST is named for its developers, Carlisle Adams and Stafford Tavares and is available internationally. CAST-256 was one of the Round 1 algorithms in the AES process [2, 3].

2.2 International Data Encryption Algorithm (IDEA)

IDEA algorithm takes input text of size 64 bits at a time and divide it in evenly; i.e., 64 bit plain text is divided into 4 sub-blocks, each of 16 bits in size. Following are the basic operations needed in the entire process.

Operations needed in the first 8 rounds

1. Multiplication modulo $2^{16}+1$.
2. Addition modulo 2^{16}.
3. Bitwise XOR.

Operations needed in the OUTPUT TRANSFORMATION phase

1. Multiplication module $2^{16}+1$.
2. Addition modulo 2^{16}.

The above mentioned operations are performed on 16 bit sub-blocks. For simplicity of expressing the operations, we denote, Multiplication modulo $2^{16}+1$ by * symbol, and Addition modulo 2^{16} by, + symbol. And bitwise XOR will be represented by its usual symbol. Using 25-bit circular left shift operation on the original key, other subsequent sub-keys are produced, used in different rounds. For instance, among the total no. of 52 keys- Sub-key K1 is having first 16bits of the original key, sub-key K2 is having the next 16 bits, and so on till sub-key K6. For ROUND1, sub-keys K1 to K6 use first (16x6=) 96 bits of the original cipher key. In ROUND2, sub-key K7 & K8 take the rest of the bits (bits 97 to 128) of the original cipher key. Then we perform circular left shift (by 25bits) operation on the original key. As a result the 26th bit of the original key shifted to the first position and becomes the first bit (of the new shifted key) and the 25th bit of the original key, moves to the last position and becomes the 128th bit (after first shift). This process continues till ROUND8, and also in the OUTPUTPUT TRANSFORMATION phase; i.e., after the ROUND8, the key is again shifted left by 25 bits and the first 64 bits of the shifted key is taken for use, and used as sub-keys K49 to K52 in the OUTPUT TRANSFORMATIONMATION phase[4-6].

2.3 Rivest Cipher (RC)

RC algorithms were first invented by Ron Rivest. "RC" stands for Rivest Cipher. The RC algorithms are widely deployed in many networking applications because of their favorable speed and variable key-length capabilities [7].

RC1

RC1 was never published. It was the first step which Rivest took in order to proceed with designing a series of symmetric key algorithms popularly known as the Rivest Cipher Algorithms. Later, different variants were designed and continuous research has been carried out by the researchers. The main idea of research was to design a Symmetric Key encryption algorithm that could be used by the users to protect their data as it passes through the network.

RC2

It is a block encryption algorithm, developed in 1987. It was considered as a proposal for the DES replacement. It is a secret key block encryption algorithm which uses a variable size key from 1 byte to 128 bytes. It consists of input and output block size

of 64-bit each. This algorithm was designed to be easily implemented on 16-bit microprocessors. If the key encryption has been performed, then this algorithm runs twice as fast as DES. The algorithm itself involves 3 further sub algorithms viz. Key Expansion, Encryption, and Decryption. This was designed as a proposal to replace the existing DES Algorithm [8].

RC3

RC3 was broken before ever being used. When the RC3 algorithm was being developed at RSA security, It was broken at the same time. Hence, it was not used.

RC4

RC4 is a stream cipher, symmetric key encryption algorithm. The same algorithm is used for both encryption and decryption. The data stream is simply XORed with the series of generated keys. The key stream does not depend on plaintext used at all. A variable length key from 1 to 256 bit is used to initialize a 256-bit state table. Vernam stream cipher is the most widely used stream cipher based on a variable key-size. It is popular due to its simplicity. It is often used in file encryption products and secure communications, such as within SSL. The WEP (Wireless Equivalent Privacy) protocol also used the RC4 algorithm for confidentiality[9, 10].

A stream cipher using variable-sized keys; it is widely used in commercial cryptography products, although it can only be exported using keys that are 40 bits or less in length. RC4 is a stream cipher, symmetric key algorithm. The same algorithm is used for both encryption and decryption as the data stream is simply XORed with the generated key sequence. The key stream is completely independent of the plaintext used. It uses a variable length key from 1 to 256 bit to initialize a 256-bit state table. The state table is used for subsequent generation of pseudo-random bits and then to generate a pseudo-random stream which is XORed with the plaintext to give the ciphertext. The algorithm can be broken into two stages: initialization, and operation. In the initialization stage the 256-bit state table, S is populated, using the key, K as a seed. Once the state table is setup, it continues to be modified in a regular pattern as data is encrypted.

The steps for RC4 encryption algorithm is as follows:

1- Get the data to be encrypted and the selected key.

2- Create two string arrays.

3- Initiate one array with numbers from 0 to 255.

4- Fill the other array with the selected key.

5- Randomize the first array depending on the array of the key.

6- Randomize the first array within itself to generate the final key stream.

7- XOR the final key stream with the data to be encrypted to give cipher text.

It was also used by many other email encryption products. The cipher can be expected to run very quickly in software. It was considered secure until it was vulnerable to the BEAST attack.

RC5

RC5 is a 32/64/128-bit block cipher developed in 1994. It was designed by Ronald Rivest for RSA Data Security (now RSA Security) in December of 1994. It is a symmetric block cipher having a variable number of rounds, word size and a secret key. It uses data-dependent operations heavily. It is a simple algorithm which has a low memory requirement. It is suitable for hardware or software. It is fast and also provides security if suitable parameters are chosen. This algorithm makes use of magic numbers. Due to the data-dependent rotations, differential cryptanalysis and linear cryptanalysis is not possible. The key used is strong if it is long. However, if the key size is short, then the algorithm is weak [11].

RC6

It was an AES finalist developed in 1997. It is a block cipher which uses 128 bit block size and supports key sizes of 128, 192 and 256 bits. It was designed in order to meet the requirements of the AES. It is an

improvement of the RC5 Algorithm. It provides even better security against attacks which may be possible in the RC5 Algorithm. It makes use of 4 registers (Each one of 32 bit) and is more secure than the RC5. It is also protected from various other possible security attacks. It uses fewer rounds and offers a higher throughput [12].

RC7

To improve the encryption efficiency of the already existing RC6 algorithm [13], RC7 has been proposed which takes relatively less time to encrypt data and is comparatively more flexible. Instead of four working registers, RC7 makes use of six such registers which makes it a better alternative to RC6 [14].

2.4 Camellia

A secret-key, block-cipher crypto algorithm developed jointly by Nippon Telegraph and Telephone (NTT) Corp. and Mitsubishi Electric Corporation (MEC) in 2000. Camellia has some characteristics in common with AES: a 128-bit block size, support for 128, 192, and 256 bit key lengths, and suitability for both software and hardware implementations on common 32-bit processors as well as 8-bit processors (e.g., smart cards, cryptographic hardware, and embedded systems). Camellia was jointly developed by Nippon Telegraph and Telephone Corporation and Mitsubishi Electric Corporation in 2000. Camellia specifies the 128-bit block size and 128-, 192-, and 256-bit key sizes, the same interface as the Advanced Encryption Standard (AES). Camellia is characterized by its suitability for both software and hardware implementations as well as its high level of security. From a practical viewpoint, it is designed to enable flexibility in software and hardware implementations on 32-bit processors widely used over the Internet and many applications, 8-bit processors used in smart cards, cryptographic hardware, embedded systems, and so on. Moreover, its key setup time is excellent, and its key agility is superior to that of AES. Camellia has been scrutinized by the wide cryptographic community during several projects for evaluating crypto algorithms. In particular, Camellia was selected as a recommended cryptographic primitive by the EU NESSIE (New European Schemes for Signatures, Integrity and Encryption) and also included in the list of cryptographic techniques for Japanese e-Government systems which were selected by the Japan CRYPTREC (Cryptography Research and Evaluation Committees).

2.5 Secure and Fast Encryption Routine (SAFER)

Secret-key crypto scheme designed for implementation in software. Versions have been defined for 40, 64, and 128 bit keys. SAFER K-64 stands for Secure and Fast Encryption Routine with a Key of 64 bits. There are no patent, copyright or other restrictions on its use. The algorithm has a block and key size of 64 bits. It is not a Feistel network like DES, but an iterated block cipher: The same function is applied for some number of rounds. Each round uses two 64-bit sub keys, and the algorithm only uses operations on bytes.

SAFER K-64 is an integrated cipher in the sense that encryption is performed by applying the same transformation repeatedly for r rounds, then applying an output Transformation; r = 6 is recommended but larger values of r can be used if desired for even greater security. Each round uses two 8-byte (64-bit) subkeys determined by a key schedule from the secret 8-byte user-selected key. The output transformation uses another 8-byte subkey determined by the key schedule. One unusual feature of SAFER K-64 is that, in contrast to most recently proposed iterated block ciphers, encryption and decryption are slightly different (i.e., they differ by more than just the reversal of the key schedule).
This algorithm uses only byte operations in the processes of encryption and decryption, which makes

it particularly useful in applications such as smart cards where very limited processing power is available. Some bit-level rotations of bytes are used in the key schedule, but this is done "once and for all", i.e., until the user-selected key is changed. To achieve security with such simple processing, SAFER K-64 exploits following two new cryptographic concepts:
(1) an unorthodox linear transform, which we call the Pseudo-Hadamard Transform (PHT), that allows the cipher rapidly to achieve the desired "diffusion" of small changes in the plaintext or the key over the resulting ciphertext [It is usually the case in block cipher design that one struggles to obtain such diffusion by carefully selecting permutations to imbed within the cipher and then doing massive statistical testing to see which ones give acceptable diffusion. As will be seen, the PHT provides a systematic way to ensure that the cipher provides the necessary diffisuion--in fact, the diffusion provided by the PHT appears to be better than that in any other cipher that we know and
(2) the use of additive key biases that eliminate the "weak keys" that plague most block ciphers. SAFER K-64 includes a recursive procedure for generating these key biases that is easy to implement and that provides the very "random" biases desired [15].

III. COMPARISON OF SYMMETRIC KEY ALGORITHMS

	CAST -256	**IDEA**	**RC-6**	**Camellia**	**SAFER**
Key Length	128,160, 192, 224 or 256	128	128,192 or 256	128, 192, 256	64
Block Size	128	64	128	128	64
Rounds	48	8.5	20	18 or 24	8

IV.CONCLUSION

Internet applications are growing very fast, so there is a need to protect such applications. Cryptographic algorithms play a main role in information security systems. In this paper a comparative study between CAST, IDEA, RC, Camellia and SAFER were presented into three factors, which are key length, block size, and number of rounds. From the study it is clear that, CAST-256 is found to be more secured as it requires more rounds the other compared algorithms.

V. REFERENCES

[1]. William Stalling “Cryptography and network security” Pearson education, 2nd Edition.
[2]. H B. Pethe, Dr. S. R. Pande “Implementation of Advanced Encryption Standard Algorithm” International Journal of Computer Science and Information Technologies, Vol. 7 (4) , 2016, 1868-1871.
[3]. Rishabh Jain, Rahul Jejurkar, Shrikrishna Chopade, Someshwar Vaidya, Mahesh Sanap “AES Algorithm Using 512 Bit Key Implementation for Secure Communication” International Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 3, March 2014 ISSN(Online): 2320-9801 ISSN (Print): 2320-9798
[4]. Sandipan Basu, "INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) – A TYPICAL ILLUSTRATION" Journal of Global Research in Computer Science Volume 2, No. 7, July 2011 ISSN: 2229-371X.
[5]. Harivans Pratap Singh et al, "Secure-International Data Encryption Algorithm" International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 2, Issue 2, February 2013 ISSN (Print) : 2320 – 3765 ISSN (Online) : 2278 – 8875.

[6]. Snehal Patil et al, "An Enhancement In International Data Encryption Algorithm For Increasing Security" International Journal of Application or Innovation in Engineering & Management (IJAIEM) Volume 3, Issue 8, August 2014 ISSN 2319 - 4847.

[7]. Sheetal Charbathia and Sandeep Sharma, "A Comparative Study of Rivest Cipher Algorithms" International Journal of Information & Computation Technology.ISSN 0974-2239 Volume 4, Number 17 (2014), pp. 1831-1838.

[8]. MILIND MATHUR, AYUSH KESARWANI, "COMPARISON BETWEEN DES , 3DES , RC2 , RC6 , BLOWFISH AND AES" Proceedings of National Conference on New Horizons in IT - NCNHIT 2013.

[9]. Allam Mousa et al, "Evaluation of the RC4 Algorithm for Data Encryption" International journal of Computer Science and Applications, Volume 3, No 2, June 2006.

[10]. P. Prasithsangaree, P. Krishnamurthy, "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs" GLOBECOM 2003.

[11]. Vikas Tyagi, Shrinivas Singh, "ENHANCEMENT OF RC6 (RC6_EN) BLOCK CIPHER ALGORITHM AND COMPARISON WITH RC5 & RC6" Journal of Global Research in Computer Science Volume 3, No. 4, April 2012 ISSN:2229-371X.

[12]. P.Sritha1, R.Ashokkumar et al, "A new modified RC6 algorithm for cryptographic applications" International Journal of Advanced Research in Computer and Communication Engineering Vol. 3, Issue 12, December 2014 ISSN (Online) : 2278-1021 ISSN (Print) : 2319-5940.

[13]. T. Shimoyama, K. Takeuchi and J. Hayakawa, “Correlation Attack to the Block Cipher RC5 and the Simplified Variants of RC6”, 3rd AES Conference, (2004).

[14]. Rashmi, Vicky Chawla et al, "The RC7 Encryption Algorithm" International Journal of Security and Its Applications Vol. 9, No. 5 (2015), pp. 55-60.

[15]. James L. Massey , "SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm" Reprinted from Fast Software Encryption (Ed. R. Anderson), Lecture Notes in Computer Science No. 809. New York: Springer, 1994, pp. 1-17.