A Comparative Analysis on Symmetric Key Encryption Algorithms

G. Muthukumar
Research scholar
School of Computer Science And Engineering, Bharathidasan University, Trichy-23.

Dr. E. George Dharma Prakash Raj
Assistant professor
School of Computer Science And Engineering, Bharathidasan University, Trichy-23.

Abstract - **Nowadays, the use of internet are growing increasingly across the world, security becomes a prime concern of issue for the society. Earlier security was a major issue for military applications but now the area of applications has been enhanced since most of the communication takes place over the web. Cryptography is an area of computer science which is developed to provide security for the senders and receivers to transmit and receive confidential data through an insecure channel by a means of process called Encryption/ Decryption. Cryptography ensures that the message should be sent without any alterations and only the authorized person can be able to open and read the message. A number of cryptographic techniques are developed for achieving secure communication. There are basically two techniques of cryptography- Symmetric and Asymmetric. This paper provides a fair comparison between Five most common symmetric key cryptography algorithms: Blowfish, Two fish, Three fish, RC2, RC5.**

Keywords: **Cryptography, Symmetric key encryption, Blowfish, Two fish, Three fish, RC2, RC5.**

I. INTRODUCTION

Cryptography [1] is the science of devising methods that allow information to be sent in a secure form in such a way that the only person able to retrieve this information is the intended recipient. The highly use of networking leads to the data exchange over the network while communicating to one and another system. While communication it is very important to encrypt the message so that intruder cannot read the message. Network security is highly based on cryptography. Cryptography is an art of hiding information by encrypting the message using algorithms. The cryptography system is a system which performs encryption and decryption process. The encryption process takes plain text as input and produce an output called cipher text using keys. The decryption process performs same as encryption but in reverse order.

Cryptography algorithm mainly falls under two categories i.e. Asymmetric and Symmetric encryption techniques.. A plain text is encrypted using an algorithm called “encryption algorithm”. A cipher text is decrypted using an algorithm called “decryption algorithm”. A key is used at the time of encryption and decryption process. The security level of cryptography is determined by the key space (size of key).

A. Basic Terms Used in Cryptography:

1. Plain Text

The original message is used to communicate with the other is defined as plain text. E.g. Alice send ―Hello‖ message to Bob. Here, ―Hello‖ is a plain text message.

2. Cipher Text

The meaningless message is called as cipher text. In cryptography, the original message is converted into non readable message. E.g. ―Pja734‖ is a cipher text produced.

3. Encryption

Encryption is a process of converting plain text into cipher text. Encryption techniques are used to send secret message through an insecure channel.

Encryption process requires an encryption algorithm and a key. Encryption takes place at the sender side.

4. Decryption

Decryption is the reverse process of encryption where it converts text into plain text. Decryption takes place at receiver side to obtain the original message from non readable message. Decryption process requires decryption algorithm and a key.

5. Key

A key is a numeric or alpha numeric text. The key is used when encryption takes place on the plain text and at the time of decryption on the cipher text. In cryptography, selection of key is very important since the security of encryption algorithm depends on it.

B. Purpose of Cryptography:

Cryptography provides a number of security goals to provide protection to data. Following are the goals of cryptography.

1.1. Confidentiality

Information in computer is transmitted and has to be accessed only by the authorized party and not by anyone else.

1.2. Authentication

The information received by any system has to check the identity of the sender that whether the information is arriving from a authorized person or a false identity.

1.3. Data Integrity

Ensuring the information has not been altered by unauthorized or unknown that means no one in between the sender and receiver are allowed to alter the given message.

1.4. Non Repudiation

Prevents either sender or receiver from denying a message. Thus when a message is sent, the receiver can prove that the message was in fact send by the alleged sender. Similarly, when a message is received, the sender can prove the alleged receiver in fact received the message.

1.5. Access Control

Only the authorized parties are able to access the given information.

II. OVERVIEW OF ALGORITMS

In symmetric Cryptography [2] the key used for encryption is similar to the key used in decryption. Thus the key distribution has to be made prior to the transmission of information. The key plays a very important role in symmetric cryptography since their security directly depends on the nature of key i.e. the key length etc.

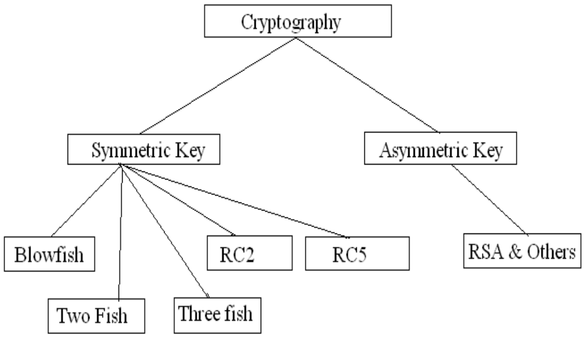

Fig.1.Classification of cryptography

The symmetric key encryption is a cryptography technique that uses a shared secret key to encrypt and decrypt the data. Symmetric encryption algorithms are very efficient at processing large amounts of information and computationally less intensive than asymmetric encryption algorithms. There are two types of symmetric encryption algorithms: stream ciphers and block ciphers which provide bit-by-bit and block encryption respectively. There are various symmetric key algorithms such as BLOWFISH, Two fish, Three fish, RC2 and RC5.

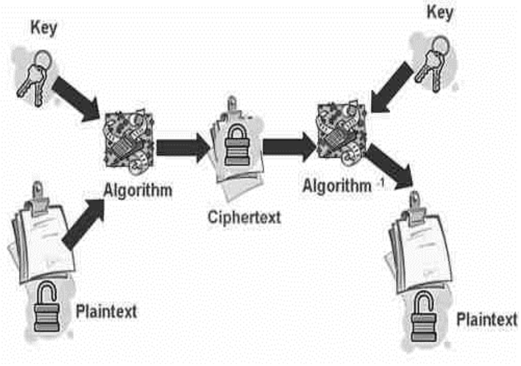

Fig.2.Symmetric key encryption

2.1. 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 by Bruce Schneier [3] as a fast, free alternative to existing encryption algorithms. Blowfish algorithm [8] 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.

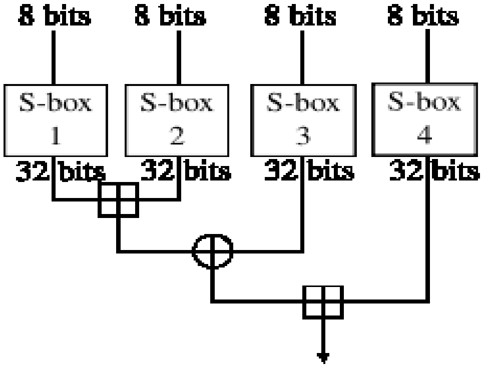

Fig.3 The round function (Feistel function) of Blowfish

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 totaling 4168 bytes.

2.2 Two fish

Two fish 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 Advanced Encryption Standard contest, but it was not selected for standardization. Two fish [4] is related to the earlier block cipher Blowfish. Two fish'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).

Two fish borrows some elements from other designs; for example, the pseudo-Hadamard transform (PHT) from the SAFER family of ciphers. Two fish has a Feistel structure like DES. On most software platforms Two fish was slightly slower than Rijndael (the chosen algorithm for Advanced Encryption Standard) for 128-bit keys, but it is somewhat faster for 256-bit keys.

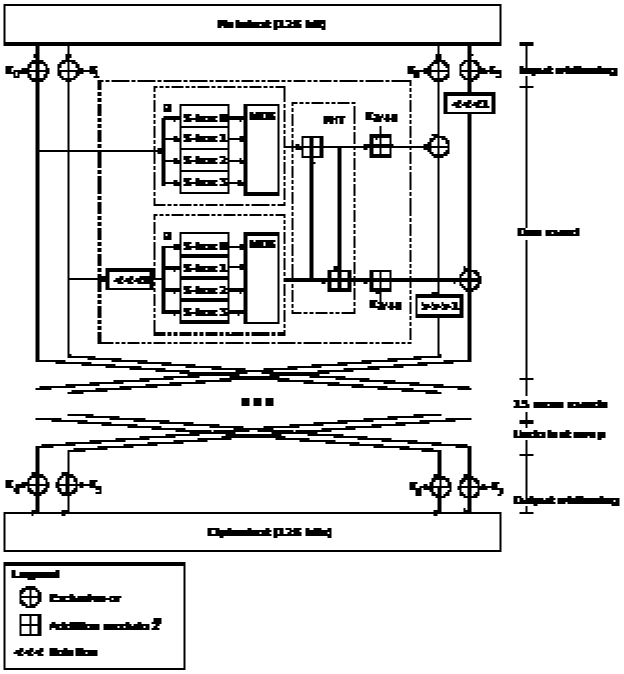

Fig.4 The Two fish algorithm

The Two fish cipher has not been patented and the reference implementation has been placed in the public domain. As a result, the Two fish algorithm is free for anyone to use without any restrictions whatsoever. It is one of a few ciphers included in the Open PGP standard (RFC 4880). However, Two fish has seen less widespread usage than Blowfish, which has been available longer.

2.3 Three fish

Three fish and the Skein hash function were designed by Bruce Schneier, Niels Ferguson, Stefan Lucks, Doug Whiting, Mihir Bellare, Tadayoshi Kohno, Jon Callas, and Jesse Walker. **Three fish** is a symmetric-key tweak able block cipher designed as part of the Skein hash function, an entry in the NIST hash function competition. Three fish uses no S-boxes or other table lookups in order to avoid cache timing attacks;[1] its nonlinearity comes from alternating additions with exclusive ORs. In that respect, it is similar to Salsa20, TEA, and the SHA-3 candidates Cube Hash and BLAKE

A related key boomerang attack [5] against a reduced round Three fish version was published. For the 32-round version, the time complexity is 2^{226}

and the memory complexity is 2^{12}; for the 33-round version, the time complexity is $2^{352.17}$with a negligible memory usage. The attacks also work against the tweaked version of Three fish: for the 32-round version, the time complexity is $2^{222}$and the memory complexity is 2^{12}; for the 33-round version, the time complexity is $2^{355.5}$with a negligible memory usage.

2.4 RC2

In cryptography, **RC2** (also known as **ARC2**) is a symmetric-key block cipher designed by Ron Rivest in 1987. "RC" stands for "Ron's Code" or "Rivest Cipher"; other ciphers designed by Rivest include RC4, RC5 and RC6.The development of RC2 was sponsored by Lotus, who were seeking a custom cipher that, after evaluation by the NSA, could be exported as part of their Lotus Notes software. The NSA suggested a couple of changes, which Rivest incorporated. After further negotiations, the cipher was approved for export in 1989. Along with RC4, RC2 with a 40-bit key size was treated favorably under US export regulations for cryptography.

Anonymously posted to the Internet on the Usenet forum, sci. crypt. Mentions of CodeView and Soft ICE (popular debuggers) suggest that it had been reverse engineered. A similar disclosure had occurred earlier with RC4.In March 1998 Ron Rivest**[6]** authored an RFC publicly describing RC2 himself.

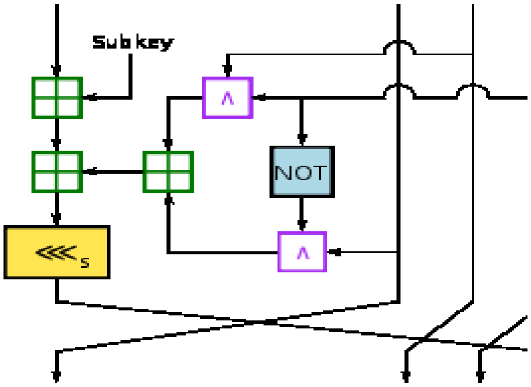

Fig.5 The MIX transformation of RC2; four of these comprise a MIXING round

RC2 is a 64-bit block cipher with a variable size key. Its 18 rounds are arranged as a source-heavy Feistel network[8], with 16 rounds of one type (*MIXING*) punctuated by two rounds of another type (*MASHING*). A MIXING round consists of four applications of the MIX transformation, as shown in the diagram.RC2 is vulnerable to a related-key attack using 2^{34} chosen plaintexts (Kelsey et al., 1997)

2.5 RC5

In cryptography, **RC5** is a symmetric-key block cipher notable for its simplicity. Designed by Ronald Rivest in 1994,[7] *RC* stands for "Rivest Cipher", or alternatively, "Ron's Code" (compare RC2 and RC4). The Advanced Encryption Standard (AES) candidate RC6 was based on RC5. 12-round RC5 (with 64-bit blocks) is susceptible to a differential attack using 2^{44} chosen plaintexts. 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.

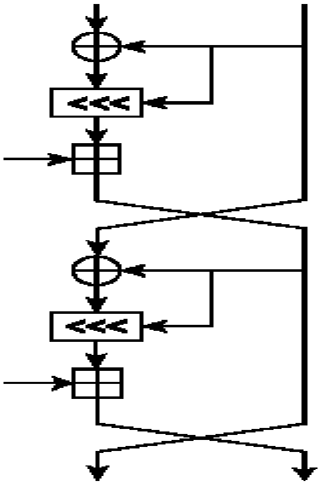

Fig.6 One round (two half-rounds) of the RC5 block cipher

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-network[8]. The encryption and decryption routines can be specified in a few lines of code. The tantalizing simplicity of the algorithm together with the novelty of the data-dependent rotations has made RC5 an attractive object of study for cryptanalysts. The RC5 is basically denoted as RC5-w/r/b where w=word size in bits, r=number of rounds, b=number of 8-bit byte in the key.

III. COMPARISON OF SYMMETRIC KEY ALGORITMS

Table 1. Comparison of table

Factors	**Blow fish**	**Two fish**	**Three fish**	**RC2**	**RC5**
Designers	Bruce Schneier	Bruce Schneier	Bruce Schneier, Stefan lucks & Others	Ron Rivest	Ron Rivest
First Published	1993	1998	2008	1996	1994
Related to	Two fish	Three fish	Blow fish, Two fish	RC4	RC6
Key Size	32-448 Bits (128 by default)	128, 192, or 256 bits	256, 512, or 1024 bits	8-1024 bits (64 by default)	0-2040 bits (128 suggested)
Block size	64 bits	128 bits	256, 512, or 1024 bits	64 bits	32,64, or 128 bits (64 suggested)
Rounds	16	16	72	16 of type MIXING, 2 of type MASHING	1-255 (12 suggested)
Algorithm Structure	Feistel N/w	Feistel N/w	S-box	Feistel N/w	Feistel N/w
Attacks	Not Yet	Differential (impossible)	combines rotational with Rebound	Related key	Differential

IV. CONCLUSION

This paper gives a comparative analysis of the symmetric key encryption algorithms like Blowfish, Two fish, Three fish, RC2, RC5. Among those algorithms the Three fish algorithm uses a variable number of bits ranging from 256 to 1024 bits and encrypts the data 72 times. So it is impossible for a hacker to decrypt it.

REFERENCES

[1] W. Stallings, **Cryptography and Network Security** Principles and Practices Fourth Edition, Pearson Education, Prentice Hall, 2010.

[2] Ayushi, **"A Symmetric Key Cryptographic Algorithm"** International Journal of Computer Applications (0975- 8887), Volume 1, 2010.

[3] Bruce Schneier, **" The Blowfish Encryption algorithm Retrieved"**, 2008.

[4] Bruce Schneier, **"Twofish Cryptanalysis Rumors**", Schneier on Security blog, 2005.

[5] Jiazhe Chen; Keting Jia, **"Improved Related-key Boomerang Attacks on Round-Reduced Threefish-512"**,2009.

[6] Lars R. Knudsen, Vincent Rijmen, Ronald L. Rivest, Matthew J. B. Robshaw: **On the Design and Security of RC2**. Fast Software Encryption 1998.

[7] Rivest, R. L, **"The RC5 Encryption Algorithm"** Proceedings of the Second International Workshop on Fast Software Encryption (FSE) *1994.*

[8] Bruce Scheneir, **Applied Cryptography: Protocols, Algorithms, and Source Code in C**. John Wiley & Sons, 1996.

[9] "A Survey on Symmetric Key Encryption Algorithms"- E Surya et al , International Journal of Computer Science & Communication Networks -2012.

[10]" A Survey on Various Most Common Encryption Techniques",- International Journal of Advanced Research in Computer Science and Software Engineering- Volume 2, Issue 7, July 2012.