T.Gunasundari *et al*, International Journal of Computer Science and Mobile Applications,
Vol.2 Issue. 2, February- 2014, pg. 78-83 **ISSN: 2321-8363**

A Comparative Survey on Symmetric Key Encryption Algorithms

T.Gunasundari[1], Dr. K.Elangovan[2]

[1]Research scholar, School of Computer Science and Engineering, Bharathidasan University
Tiruchirappalli-620023, India
gunavinod@gmail.com

[2]Assistant professor, School of Computer Science and Engineering, Bharathidasan University
Tiruchirappalli-620023, India
murthy.elango@gmail.com

Abstract:

Security is the most challenging aspects in the internet and network applications. Internet and networks applications are growing very fast, so the importance and the value of the exchanged data over the internet or other media types are increasing. Hence the search for the best solution to offer the necessary protection against the data intruders' attacks along with providing these services in time is one of the most interesting subjects in the security related communities. Cryptography is the one of the main categories of computer security that converts information from its normal form into an unreadable form. The two main characteristics that identify and differentiate one encryption algorithm from another are its ability to secure the protected data against attacks and its speed and efficiency in doing so. There are basically two techniques of cryptography-Symmetric and Asymmetric .This paper provides a fair comparison between four most common symmetric key cryptography algorithms: RC2, RC4, RC5, and RC6.

Keywords*:* Cryptography, Symmetric key encryption, RC2, RC4, RC5, RC6.

I. INTRODUCTION

Cryptography is a science of secret writing. It is the art of protecting the information by transforming it into an unreadable format in which a message can be concealed from reader and only the intended recipient will be able to convert it into original text. Its main goal is to keep the data secure from unauthorized access. Data can be read and understood without any special measure is called plaintext. The method of disguising plaintext in such a way as to hide its substances is called encryption. Encrypting plaintext results in unreadable gibberish called cipher text. The process of reverting cipher text to its original plaintext is called decryption. A system provides encryption and decryption is called cryptosystems. Cryptography provides number of security goals to ensure the privacy of data, on-alteration of data and so on. Due to the great security advantages of cryptography it is widely used today.

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 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 RC2, RC4, RC5 and RC6 information.

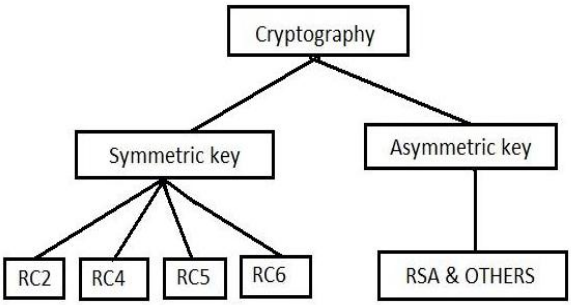

Fig.1.Classification of cryptography

II. OVERVIEW OF RC ALGORITHM

1. 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"; other ciphers designed by Rivest include RC4, RC5 and RC6.

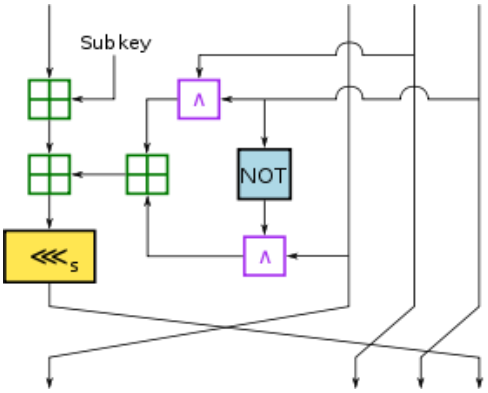

Fig.2 The MIX transformation of RC2; four of these comprise a MIXING round

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.

Initially, the details of the algorithm were kept secret — proprietary to RSA Security — but on 29 January 1996, source code for RC2 was 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 authored an RFC publicly describing RC2 himself. 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*). 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. RC4

RC4 was designed by Ron Rivest of RSA Security in 1987. While it is officially termed "Rivest Cipher 4", the RC acronym is alternatively understood to stand for "Ron's Code" (see also RC2, RC5 and RC6).

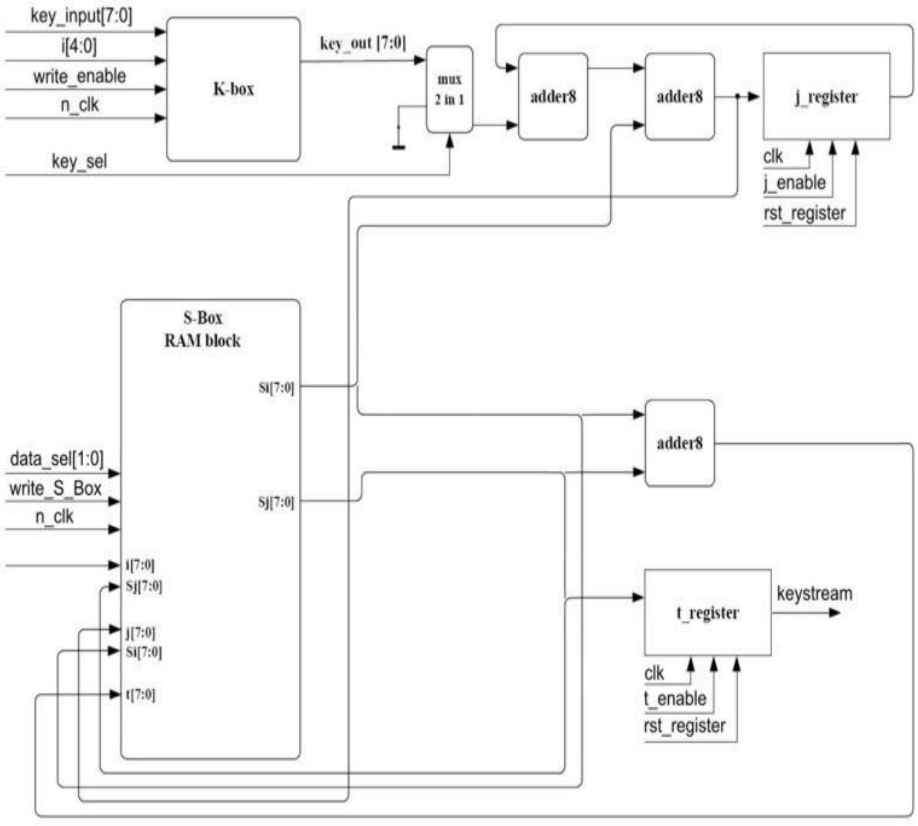

Fig.3 The MANY transformation of RC4

RC4 was initially a trade secret, but in September 1994 a description of it was anonymously posted to the Cypherpunks mailing list. It was soon posted on the sci.crypt newsgroup, and from there to many sites on the Internet. The leaked code was confirmed to be genuine as its output was found to match that of proprietary software using licensed RC4. Because the algorithm is known, it is no longer a trade secret. The name RC4 is trademarked, so RC4 is often referred to as ARCFOUR or *ARC4* (meaning alleged RC4) to avoid trademark problems. RSA Security has never officially released the algorithm; Rivest has, however, linked to the English Wikipedia article on RC4 in his own course notes. RC4 has become part of some commonly used encryption protocols and standards, including WEP and WPA for wireless cards and TLS.

3. 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" (compare RC2 and RC4). 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.

The encryption and decryption routines can be specified in a few lines of code. The key schedule, however, is more complex, expanding the key using an essentially one-way function with the binary expansions of both e and the golden ratio as sources of "nothing up my sleeve numbers". 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.

4. RC6

In cryptography, RC6 (Rivest Cipher *6*) is a symmetric key block cipher derived from RC5. It was designed by Ron Rivest, Matt Robs haw, 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.

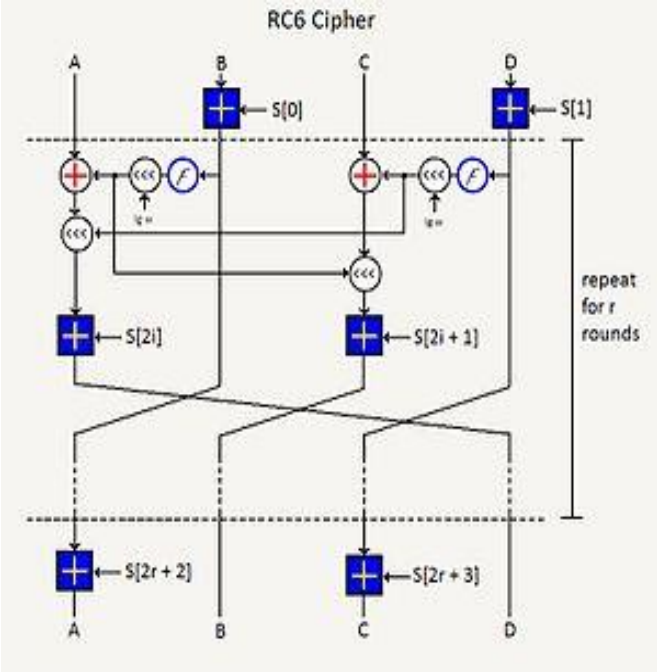

Fig.4 The MIX transformation of RC4

RC6 proper has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits, but, like RC5, it may be parameterized to support a wide variety of word-lengths, key sizes, and number of rounds. 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.

III. COMPARISON OF SYMMETRIC KEY ALGORITMS

FACTORS	RC2	RC4	RC5	RC6
Created by	Ron Rivest in 1994	Ron Rivest (RSA Security) in 1994	Ron Rivest in 1994	Yiqun Lisa Yin in 1998

Block size	64	2,064 bits (1,684 effective)	32, 64 or 128 bits	128 bits
Key Length	8–1024 bits, in steps of 8 bits; default 64 bits	40– 2,048 bits	0 to 2040 bits (128 suggested)	128, 192, or 256 bits
Rounds	16	256	1-255 (12 suggested originally)	20
Algorithm Structure	Source-heavy Feistel N/w	Feistel N/w	Feistel N/w	Feistel N/w
Effective Ness	Efficient in S/W	Effective in both S/W	Slow especially in S/W	Slow
Attacks	Related-key Network	Fluhrer Mantin and Shamir attack	differential attack	Brute force Attack

IV. CONCLUSION

This paper gives a detailed study of the symmetric key encryption algorithms like RC2, RC4, RC5 and RC6. Among those algorithms the RC6 algorithm uses a variable number of bits ranging from 8 to 1024 bits and encrypts the data 16 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, 2009.
[2] " **A Survey on Symmetric Key Encryption Algorithms"-** E Surya et al , International Journal of Computer Science & Communication Networks -2012 .
[3] Lars R. Knudsen, Vincent Rijmen, Ronald L. Rivest, **Matthew J. B. Robshaw: On the Design and Security of RC2. Fast Software Encryption .**
[4] Ron Rivest.**" RSA Security Response to Weaknesses in Key Scheduling Algorithm of RC4"**
[5]" **A Comparative Survey on Symmetric Key Encryption Techniques**"- Monika Agrawal et al. / International Journal on Computer Science and Engineering (IJCSE)-2008.
[6] **"On the Security of RC4 in TLS and WPA".** Information Security Group, Royal Holloway, University of London.
[7] Yukiyasu Tsunoo; Teruo Saito; Hiroyasu Kubo; Maki Shigeri; Tomoyasu Suzaki; Takeshi Kawabata (2005), **The Most Efficient Distinguishing Attack on VMPC and RC4A**.
[8] Biryukov A. and Kushilevitz E.Improved **Improved Cryptanalysis of RC5. EUROCRYPT .**
[9] R.L. pavan, M.J.B. Robshaw, R.Sidney, and Y.L. Yin. **The RC6 Block Cipher**..
[10] Rivest, R. L. (1994). **"The RC5 Encryption Algorithm"** (*Proceedings of the Second International Workshop on Fast Software Encryption (FSE) 1994.*

