International Journal of Information & Computation Technology.
ISSN 0974-2239 Volume 4, Number 17 (2014), pp. 1831-1838

http://www. irphouse.com

# A Comparative Study of Rivest Cipher Algorithms

**Sheetal Charbathia and Sandeep Sharma**

*Guru Nanak Dev University, Punjab, India*

**Abstract**

The purpose of an encryption algorithm is to provide security of data. If an encryption algorithm cannot be broken easily, then it is said to be secure. The ultimate goal is to protect data against any unauthorized access or theft. In this paper, a comparative study has been done against a family of symmetric key algorithms called the Rivest Cipher algorithms to get a hold on various security goals that the algorithms intends to provide. All the Rivest Cipher Algorithms have been described briefly with the basic working principle and other useful details. And lastly, a comparison of these algorithms considering the different parameters has been done in order to see how each version of the algorithm was different from the other and how improvements were incorporated. Due to the increasing computing power, the RC6 algorithm is vulnerable to attacks. Some measures should can be taken to protect RC6 algorithm against any threat so that this algorithm can be secure for decades and more. This can be done by modifying this algorithm further.

**Keywords—** cryptography, symmetric key cryptography, asymmetric key cryptography, hash function cryptography, RC2, RC4, RC5, RC6

## Introduction

The growing use of networks has made us concern for security. Security provides protection against unwanted behavior. The communication network is like a platform for malicious users and other intruders who try to intercept or even harm the information that is communicated via the network. To protect the information from being leaked, it is necessary to send it in a form which is unreadable. For providing such security, cryptography comes into play.

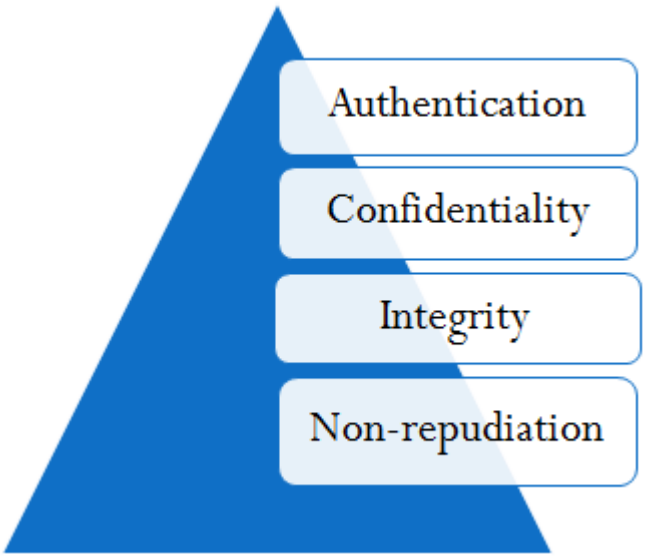


**Fig. 1 Goals of security**

The various goals of security are:

- **Authentication:** The process of proving one's identity.
- **Confidentiality:** It ensures that the message can only be read by the intended receiver.
- **Integrity:** It assures the receiver that the message that has been received, unaltered.
- **Non-repudiation:** The sender cannot deny having sent the message and also the receiver cannot deny having received the message.

Cryptography is the art or science of secrecy. It is about communicating securely through insecure channels. It not only protects the data from alterations and theft, but also provides user authentication. There are three types of cryptographic schemes which have been discussed below. The initial data or normal text is referred to as plaintext. When this plain text is encrypted, it is called as ciphertext. This ciphertext, when decrypted will again turn into usable plaintext.

**Symmetric Key Cryptography**

In this scheme, the keys used for encryption and for decryption are the same. The secret key should be known to both the sender as well as the receiver. The difficulty in this approach arises in the distribution of the key. It is generally categorized as being either stream ciphers or block ciphers.

**Stream ciphers** operate on a single bit (byte or computer word) at a time.. A **block cipher** encrypts one block of data at a time. It can be in Electronic Code Book mode (ECB),  Cipher Block Chaining mode (CBC), Output Feedback mode (OFB),

Cipher Feedback mode (CFB),  Counter mode (CTR), Galois Counter Mode (GCM).Various algorithms which fall under the category of Symmetric key cryptography are:RC2, RC4, RC5, RC6, AES, DES, 3DES, Blowfish, Twofish, Serpant, CAST5, CAST128, SEED, IDEA, TEA, XTEA, DEAL, FROG, Simon, Speck

**Asymmetric Key Cryptography**

In this scheme, the keys used for encryption and decryption purpose are different from each other. This technique is also known as Public Key Cryptography. The data is encrypted using a public key whereas the decryption can be done only by the private key. Public Key Cryptography depends upon mathematical functions/one-way functions, which are easy to compute but it is difficult to compute their inverse function. A disadvantage of PKC is that it is slower than the symmetric key cryptography. Various algorithms which fall under the category of Asymmetric key cryptography are: RSA, DSA, YAK, Diffie Hellman, ElGamal, Merkle's Puzzles, ECC

**Cryptography Using Hash Function**

In this, a cryptographic hash function is used in order to transform a large block of a string of data to a small block of data. This is a one way function. So, it means that the transformation is done in a way so that recreation of that original data is difficult or say impractical. Further, it is also difficult to find two strings which may be transformed to the same hash. Algorithms under this category are: MD2, MD4, MD5, SHA-0, SHA-1, SHA-3, GOST, HAVAL, RIPEMD, RIPEMD-128/256, RIPEMD-160, RIPEMD-320, Tiger(2), Whirlpool, RTR0

This paper limits the discussion to the family of Rivest Cipher Algorithms. RC algorithms belong to a family of symmetric-key encryption algorithms. They 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. There are mainly six RC algorithms that have been designed so far out of which only four exist.

**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 beforehand, then this algorithm runs twice as fast as DES on an IBM AT. 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.

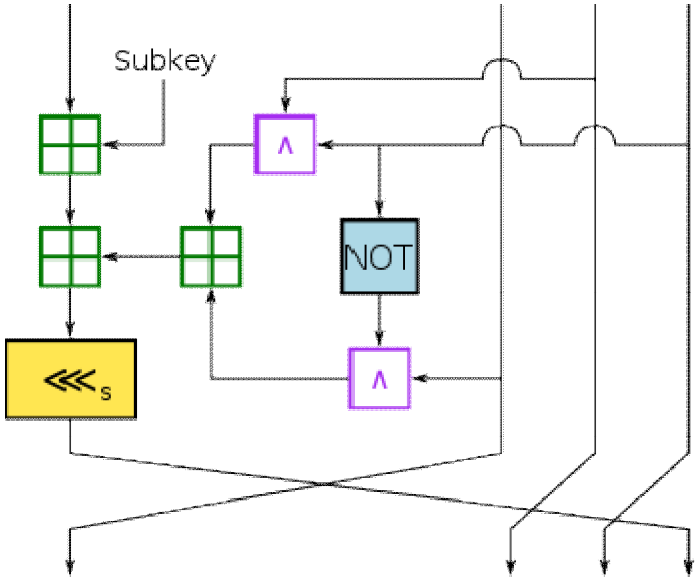


**Fig. 2 MIX transformation of RC2** [11]

**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. 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.

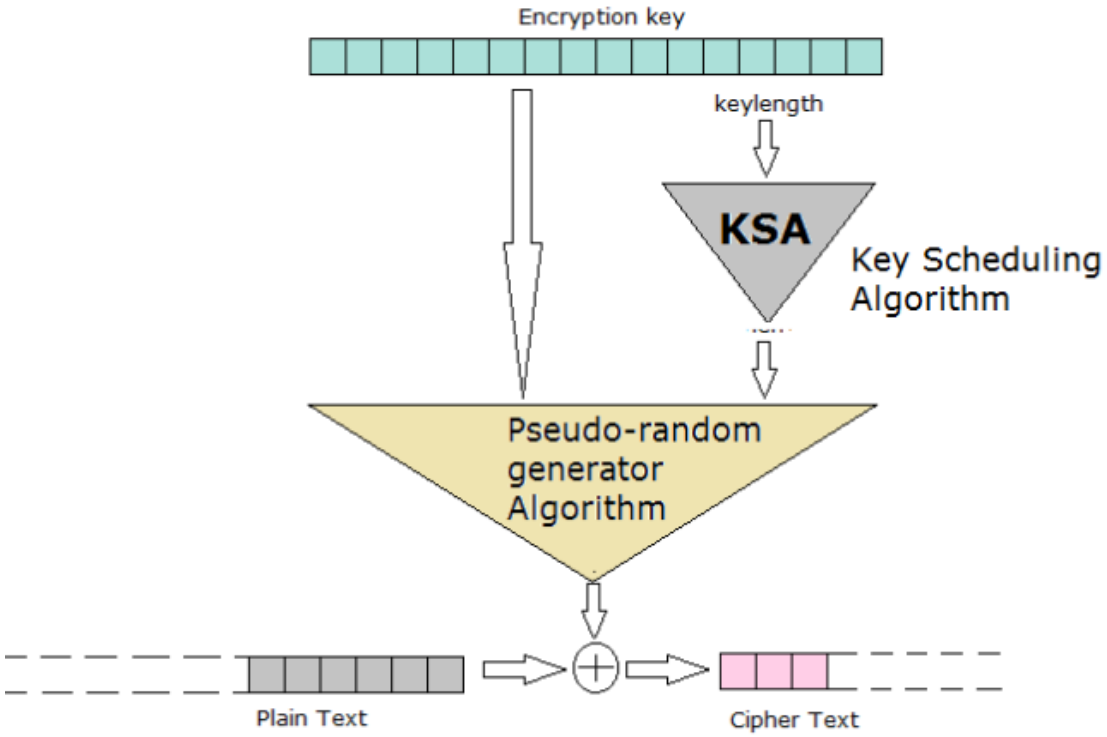


**Fig. 3 Schematic representation of RC4** [12]

**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.

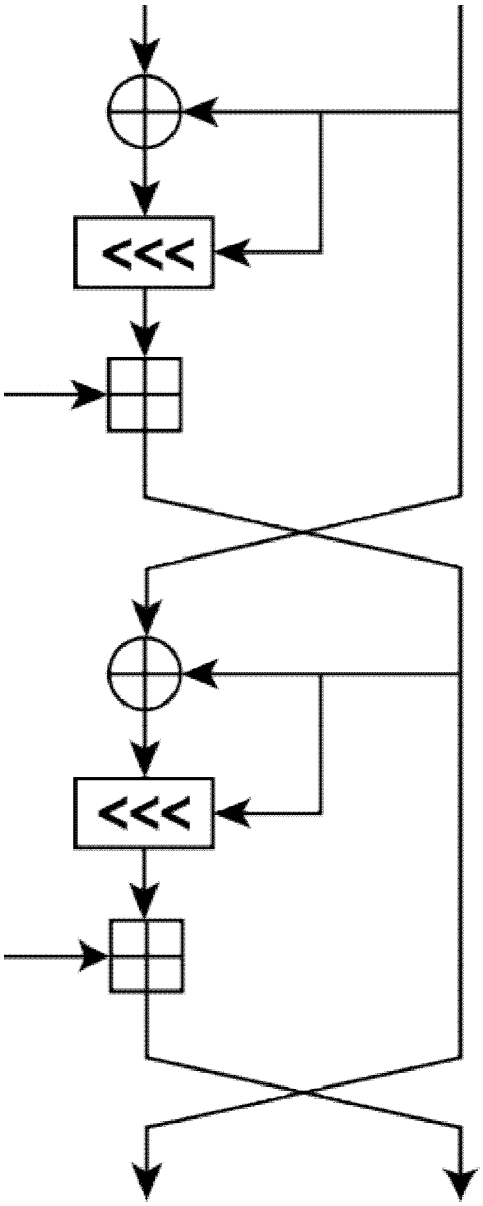


**Fig. 4 One round of RC5 block cipher [13]**

**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.

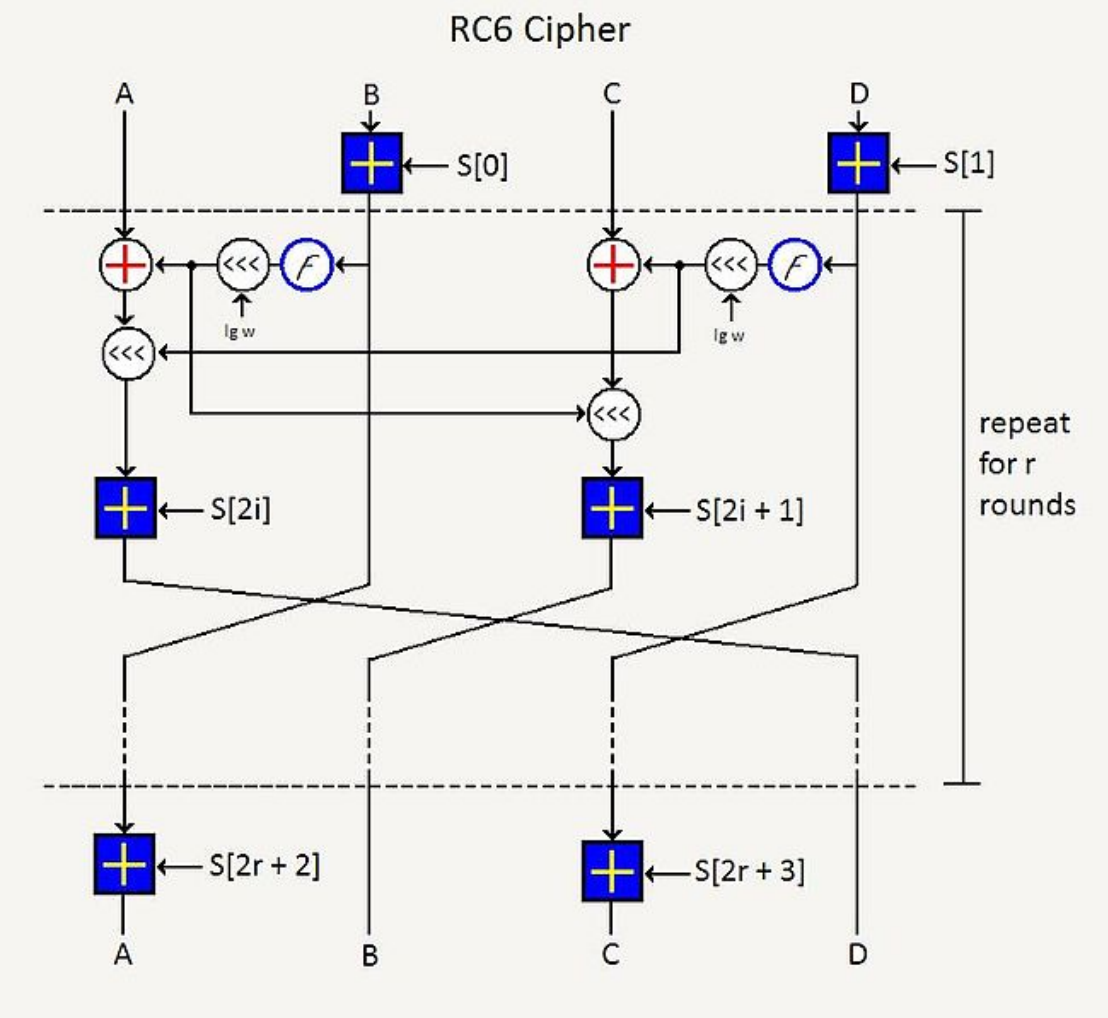


**Fig. 5 MIX Transformation of RC6** [14]

**TABLE 1. Comparison between RC Algorithms**

| **Algorithm** | RC2 | RC 4 | RC 5 | RC 6 |
|---|---|---|---|---|
| **year** | 1987 | 1987 | 1994 | 1998 |
| **cipher** | block | stream | block | block |
| **Block size** | 64 | 2064 | 32, 64, 128 | 128, 256 |
| **Key size** | 8-128 default 64 | 1-256 | 0-2048 | 128, 192, 256 |
| **Rounds** | 16 | 256 | 0-255 | 20 (recommended) |
| **Possible Attacks** | Differential, Linear | BEAST | Differential | Correlation |
| **Security** | vulnerable | vulnerable | vulnerable | Considered vulnerable |
| **Possible keys** | $2^{64}$, $2^{128}$ | …… | ……. | $2^{128}$, $2^{192}$, $2^{256}$ |
| **Operations used** | +, -, &, ~, ror, rol | +, mod, xor | +, -, <<<, >>>, xor, mod | +, -, *, <<<, >>>, xor, mod |

## CONCLUSION

There are many Symmetric key cryptography algorithms which have been proposed. The Rivest Cipher Algorithm is one among those. Different versions of this algorithm have been released. In this paper, a comparative study of the various Rivest Cipher Algorithms has been done. The RC6 algorithm although is not found vulnerable to any practical attack, while some theoretical attacks still exist. Nowadays, as computing power is increasing, RC6 could be broken in some years. So, the need for a stronger algorithm arises. Therefore, the algorithm should be improved in order to make it safe against security attacks.

## REFERENCES

[1] R. Rivest, ” rfc 2268’’ MIT Laboratory for Computer Science, Category: Informational and RSA Data Security, Inc. March 1998
[2] Allam Mousa and Ahmad Hamad, "Evaluation of RC4 Algorithm for Data Encryption", International Journal of Computer Science & Applications, vol-3, No.2, June 2006.
[3] Jian Xie, Xiaozhong Pan, “An Improved RC4 Stream Cipher”, International Conference on Computer Application and System Modeling, ISBN 978-1-4244-7237-6, IEEE 2010.
[4] Ronald L.Rivest. “The RC5 Encryption Algorithm”, Proceedings of the 1994 Leuven Workshop on Fast Software Encryption, Springer Berlin Publishers, vol. 1008, pp. 86-96, 1995.
[5] Ronald L. Rivest, M.J.B. Robshaw, R. Sidney, and Y.L. Yin, “The RC6 Block Cipher”, M.I.T. Laboratory for Computer Science, RSA Laboratories. August 1998.
[6] Praveen Gauravaram, Lars R. Knudson, Peter Staroulakis, Mrk Stamp(Eds.), “Cryptographic Hash functions”, Handbook of Information and Communication Security, Springer 2010.
[7] Iris Anshel, Dorian Goldfeld, Cryptographic hash function, US 20140019747 A1, 2014.
[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] An Overview of Cryptography, Gary C. Kessler, 2 May 2014
[10] The Security of the RC6 Block Cipher, Scott Contini, Ronald L. Rivest, M.J.B. Robshaw et. Al, Version 1.0 - August 20, 1998
[11] Mix Transformation of RC2, Wikipedia.org. File:RC2 InfoBox Diagram.svg
[12] Schematic Representation of RC4:RedHat Security blog
[13] One round of RC5 block Cipher, File:RC5 InfoBox Diagram.svg
[14] Fiestel function of RC6 Algorithm, File:RC6 Cryptography Algorithm.jpg