International Journal of Security and Its Applications
Vol. 9, No. 5 (2015), pp. 55-60
http://dx.doi.org/10.14257/ijsia.2015.9.5.05

The RC7 Encryption Algorithm

Rashmi[1], Vicky Chawla[2], Rajni Sehgal[3] and Renuka Nagpal[4]

[1,2]Student, Dept. of Computer Science & Engineering, Amity University, Uttar Pradesh
[3,4]Assistant Professor, Dept. of Computer Science & Engineering, Amity University, Uttar Pradesh
[1]rashmikr1993@gmail.com, [2]chawlavicky497@gmail.com
[3]rsehgal@amity.edu, [4]rnagpal1@amity.edu

Abstract

Cryptography can be defined as the art of secret writing or protecting information by transforming it (encrypting it) into an unreadable format, called cipher text and then transmitting it across insecure networks, so that it cannot be read by anyone except the intended recipient. Only those who possess a secret key can decipher (or decrypt) the message into plain text. Encrypted information can sometimes be broken by cryptanalysis, also called code breaking, although modern cryptography techniques are virtually unbreakable. Various algorithms help achieve flawless encryption results which are mostly unbreakable. This paper is an attempt to improve one such algorithm, i.e. RC6 by adding on to its existing functionalities.

Keywords: *Cipher text, Cryptanalysis, Cryptography, Decryption, Encryption, RC6*

1. Introduction

As e-mail, chat and other forms of electronic communication become increasingly necessary by the day, it becomes all the more important to simultaneously protect and maintain the security of all the data involved in these operations. To achieve this, cryptography comes into the picture. Cryptography is achieved by using various algorithms which are based on either substitution of plain text with some cipher text, or by using certain transcription techniques, or a combination of both. Based on the type of key being used, the algorithms could be classified into Symmetric key algorithms (*e.g.*, AES, DES, RC5, Blowfish, *etc.*,) and Asymmetric key algorithms (*e.g.,* RSA, MD5, SHA, *etc.*,).

Symmetric key algorithms are those in which encryption and decryption are performed using the same key. Asymmetric key algorithms are the ones in which encryption and decryption are performed using different keys.

The RC algorithms are a set of symmetric-key encryption algorithms invented by Ron Rivest. The "RC" may stand for either Rivest's Cipher or, more informally, Ron's code. There have been six RC algorithms so far. We have proposed an improvised version of the RC-6 algorithm, namely RC-7 in our paper.

2. Related Work

RC4 is a stream cipher designed in 1987 by Ron Rivest for RSA data Security (now RSA Security) [1, 2]. It is a variable key-size stream cipher with byte-oriented operations. This algorithm is used for random permutation. RC4 is used in the Secure Sockets Layer/Transport Layer Security (SSL/TLS) standards that have been defined for communication between Web browsers and servers [3].

ISSN: 1738-9984 IJSIA

In 1995, Ronald L. Rivest described the RC5 algorithm [4], keeping in mind a number of objectives such as RC5 being a symmetric block cipher, fast, suitable for hardware and software implementation, adaptable to processors of different word-lengths, iterative in structure (with variable no. of rounds) and with variable-length cryptographic key [5]. RC5 was a parameterized algorithm which was intended to be easy to implement.

Further, in 1998, Ronald L. Rivest, M. J. B. Robshaw, R. Sidney and Y. L. Yin gave the RC6 algorithm [6], which was a new block cipher submitted to NIST for consideration as the new Advanced Encryption Standard (AES) [7, 8]. The design of RC6 began with a consideration of RC5 as a potential candidate for an [9] AES submission. Modifications were then made to meet the AES requirements, to increase security, and to improve performance [10, 11]. The inner loop however, is based around the same 'half-round' found in RC5 [12]. Like RC5, RC6 is also parameterized.

2.1 RC5 & RC6 Block Ciphers

RC6 operates on units of 4 w-bit words using the 6 operations as follows [13]:

❶ a + b: integer addition modulo 2^w
❷ a - b: integer subtraction modulo 2^w
❸ a @ b: bitwise exclusive-or of w-bit words
❹ a * b: integer multiplication modulo 2^w
❺ <<< b: rotate the w-bit word 'a' to the left by the given amount by the least significant lgw bits of b
❻ a >>> b: rotate the w-bit word a to the right by the amount given by the least significant lgw bits of b.

The two main **features** in RC6 compared to RC5 are [14, 15]:

A. Inclusion of Integer Multiplication: - It is used to increase the diffusion achieved per round so that fewer rounds were needed and the speed of cipher increased.

B. Use of 4-bit Register: - The reason for using 4-bit working registers instead of 2-bit is technical.

RC6 is a secure, compact and simple block cipher. It offers considerable flexibility and good performance [16, 17]. Its simplicity allows analysts to quickly refine and improve estimates of its security [18, 19].

Table I. Comparison between RC5 and RC6 Block Ciphers

Parameters	Algorithm type	
	RC5	RC6
W (word size in bits)	16, 32, 64	16, 32, 64
r (No. of rounds)	0, 1, 2.., 255	0, 1, 2.., 255
b (Key length) in bytes	0, 1, 2.., 255	0, 1, 2.., 255
Block size in words	2w	4W
Block size in bits	32,64, 128	64,128, 256
Max. block size in bits	128	156
No. of keys derived from key schedule	2r+2	2r+4
Transformation Function f(x)	Does not exist	x(2x+1) mod 2w
Used Operation	+, -, ⊕, <<<, >>>	+, -, *, ⊕, <<<, >>>

3. RC7 Block Cipher

To improve the encryption efficiency of the already existing RC6 algorithm [20], 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.

3.1. Algorithm

Input: Plaintext stored in six w-bit input registers "A, B, C, D, E, and F"
Number of rounds "r"
W-bit round keys "S [0 . . . 2r + 1]"
Output: Cipher text stored in A, B, C, D, E, F

Procedure:

B = B + S [0]
D = D + S [1]
F = F + S [2]
for i = 1 to r do
{
t = (B × (2B + 1)) <<<lg w
u = (D × (2D + 1)) <<<lg w
v = (F × (2F + 1)) <<<lg w
A = ((A ⊕ t) <<<u) + S [2i+1]
C = ((C ⊕ u) <<<t) + S [2i+ 2]
E = ((E ⊕ v) <<<t) + S [2i+ 3]
(A, B, C, D, E, F) = (B, C, D, E, F, A)}
A = A + S [2r - 1]
C = C + S [2r]
E = E + S [2r + 1]

4. Design

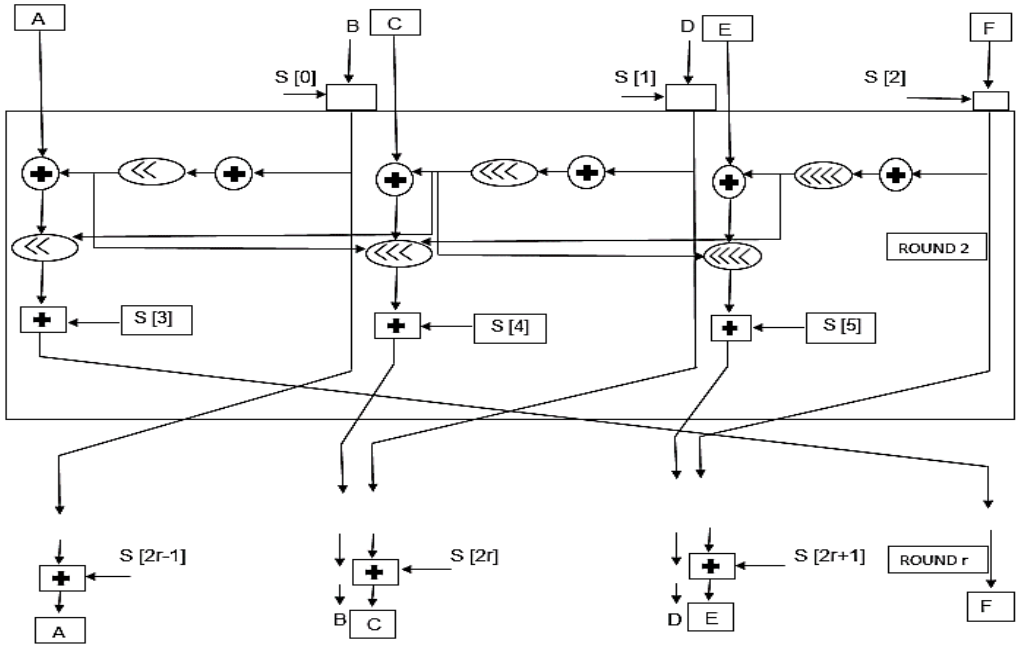

Figure 1. Design of RC7

5. Tools used

For the implementation of RC7, specifications of the computer system used are as follows:

Table II. Tools used During Study

Operating system	Windows 7
RAM	1 Gb
Processor	Intel Core i5
Hard disk	450 Gb
Text editor used	Notepad
Compiler used	Dev C++ 5.5.3

6. Results and Discussion

Table III. Comparison between RC6 and RC7

REFERENCE	**RC6**	**RC7 (Proposed)**
Plain text	00000000-00000000-00000000-00000000	00000000-00000000-00000000-00000000
Key	36a5c38f-78f7b16-4edf29c1-1ea44898	1af9897d-0a4edec3-7804776e-1ff7ae69
Cipher text	cb1bd66c-38300b19-163f8a4e-82ae9086	05bd5f8f-a85fd110-da3ffa93-c27e856e-00000000-00000000
Compilation time	0.38 seconds	0.33 seconds
Encryption time (approx.)	0.076 seconds	0.066 seconds

It is thus evident from the above results that the proposed algorithm RC7 has an encryption time less than that of RC6, thereby easier to implement and more efficient to use.

7. Conclusion

Following are the conclusions that can be drawn from our paper:-

i. Among RC6 and RC7 (proposed), the latter is found to be better owing to increased throughput, increased efficiency and decreased encryption time.

ii. RC6 also has some loopholes which can be overcome by RC7. Its advantages over RC6 are enumerated as follows:-

a. More secure and compact block cipher.
b. Offers good performance and suggestively more flexible.
c. Makes use of 6 working registers instead of 4.

d. It has a block-size of 256 bits. When using this block size, 32-bit operations are preferable given the intended architecture of AES.
e. The implementation of the cipher works according to the restrictions provided by the respective individual systems.

8. Implications of Future Research

Changing the existing modules or adding new ones can append improvements. Further enhancements can be made to the algorithm, so that it becomes more effective for encryption/decryption.

Acknowledgement

The authors express their sincere gratitude to Prof. (Dr.) Abhay Bansal, HoD, Dept. of CSE, Amity University, Uttar Pradesh for his constant guidance and attention. They are grateful to their respective parents for their valuable support and guidance throughout the course of this project. They would also like to thank the reviewers at IJSIA for their precious insights that helped them improve this paper.

References

[1] L. R. Knudsen, "Truncated and higher order differentials", Lecture Notes in Computer Science, vol. 1008, **(1994)**, pp. 196-211.
[2] B. S. Kaliski and Y. L. Yin, "Differential and linear cryptanalysis of the RC5 encryption algorithm", Lecture Notes in Computer Science, vol. 963, **(1995)**, pp. 171-184.
[3] R. L. Rivest, "The RC5 encryption algorithm", Lecture Notes in Computer Science, vol. 1008, **(1995)**, pp. 86-96.
[4] L. R. Knudsen and W. Meier, "Improved differential attacks on RC5." Advances in Cryptology Crypto'96, Lecture Notes in Computer Science, vol. 1109, **(1996)**, pp. 216-228.
[5] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems", Advances in Cryptology | Crypto '96, vol. 1109, **(1996)**, pp. 104-113.
[6] R. L. Rivest, M. J. B. Robshaw, R. Sidney and Y. L. Yin, "The RC6^{TM} Block Cipher", Advances in Cryptology | Crypto '98, Version 1.1-20th, **(1998)** August.
[7] J. Nechvatal, E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti and E. Roback, "Report on the Development of the Advanced Encryption Standard (AES)", IJSET, vol. 5, no. 18, **(2001)**.
[8] ANSI 3.106, "American National Standard for Information Systems Data Encryption Algorithm Modes of Operation," American National Standards Institute, **(1983)**.
[9] R. L. Rivest, "RC6 Block Cipher", vol. 1.1, no. 4, IJCA, **(1998)**.
[10] A. Kumar, S. Jakhar, S. Maakar, "Distinction between Secret key and Public key Cryptography with existing Glitches", IJEIM, vol. 1.1, no. 67, **(2012)**.
[11] S. Contini, R. L. Rivest, M. J. B. Robshaw and Y. L. Yin, "The Security of the RC6 Block Cipher", IJACT, Version 1.0, **(1998)** August 20.
[12] Y. Kumar and R. Munjal, "Comparison of symmetric and asymmetric cryptography with existing vulnerabilities", IJCMS, **(2011)** October.
[13] M. Marwaha, R. Bedi, A. Singh and T. Singh, "Comparative Analysis of Cryptographic Algorithms", E-ISSN 0976-3945, IJAET, **(2008)**.
[14] D. Simon, B. Aboba and R. Hurst, "The EAP-TLS Authentication Protocol", RFC 5216, **(2008)** March.
[15] P. Funk and S. Blake-Wilson, "EAP Tunneled TLS Authentication Protocol Version 1 (EAP-TTLSv1)", the Internet Society, **(2006)** March.
[16] A. Palekar, D. Simon, G. Zorn, J. Salowey, H. Zhou and S. Josefsson, "Protected EAP Protocol (PEAP) Version 2", IJAET, **(2004)** October.
[17] S. M. Seth and R. Mishra, "Comparative Analysis of Encryption Algorithms for Data Communication", IJCST, vol. 2, Issue 2, **(2011)** June.
[18] W. Diffie and M. E. Hellman, "New Direction in cryptography", IEEE Trans. Inform Theory IT, vol. 22, no. 6, **(1976)**, pp. 644-654.
[19] R. Agrawal and R. Srikant, "Fast Algorithms for Mining Association Rules", Proceedings of the 20th international conference on Very Large Databases, **(2001)**, pp. 487-499.
[20] T. Shimoyama, K. Takeuchi and J. Hayakawa, "Correlation Attack to the Block Cipher RC5 and the Simplified Variants of RC6", 3rd AES Conference, **(2004)**.

