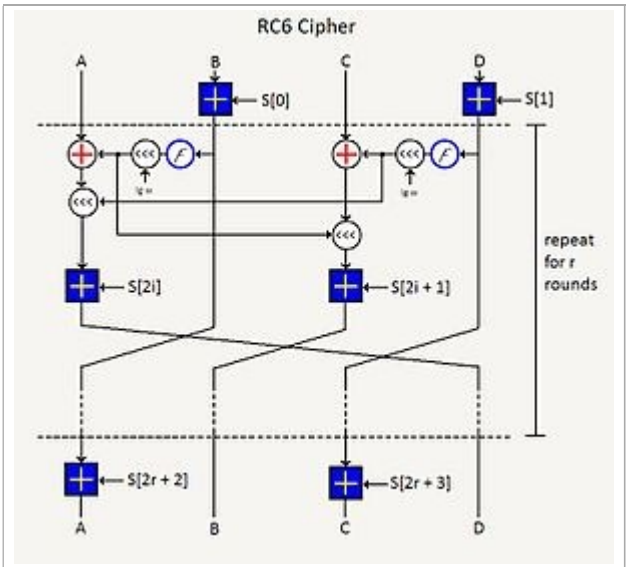
RC6

In cryptography, **RC6** (**Rivest cipher 6**) is a symmetric key block cipher derived from RC5. It was designed by Ron Rivest, Matt Robshaw, 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 was a proprietary algorithm, patented by RSA Security.

RC6 proper has a block size of 128 bits and supports key sizes of 128, 192, and 256 bits up to 2040-bits, but, like RC5, it may be parameterised 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, although 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.

Contents

RC6



The Feistel function of the RC6 algorithm.

General	
Designers	Ron Rivest, Matt Robshaw, Ray Sidney, Yiqun Lisa Yin
First published	1998
Derived from	RC5
Certification	AES finalist
Cipher detail	
Key sizes	128, 192, or 256 bits
Block sizes	128 bits
Structure	Feistel network (Type 2)[1]
Rounds	20

Encryption/decryption

Note that the key expansion algorithm is practically identical to that of RC5. The only difference is that for RC6, more words are derived from the user-supplied key.

```
// Encryption/Decryption with RC6-w/r/b
//
// Input:   Plaintext stored in four w-bit input registers A, B, C & D
//  r is the number of rounds
//  w-bit round keys S[0, ... , 2r + 3]
//
// Output: Ciphertext stored in A, B, C, D
```

```
//
// '''Encryption Procedure:'''

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

// '''Decryption Procedure:'''

    C = C - S[2r + 3]
    A = A - S[2r + 2]

    for i = r downto 1 do
    {
        (A, B, C, D) = (D, A, B, C)
        u = (D*(2D + 1)) <<< lg w
        t = (B*(2B + 1)) <<< lg w
        C = ((C - S[2i + 1]) >>> t) ⊕ u
        A = ((A - S[2i]) >>> u) ⊕ t
    }
    D = D - S[1]
    B = B - S[0]
```

Possible use in NSA "implants"

In August 2016, code reputed to be Equation Group or NSA "implants" for various network security devices was disclosed.[2] The accompanying instructions revealed that some of these programs use RC6 for confidentiality of network communications.[3]

Licensing

As RC6 has not been selected for the AES, it was not guaranteed that RC6 is royalty-free. As of January 2017, a web page on the official web site of the designers of RC6, RSA Laboratories, states the following:[4]

> "We emphasize that *if* RC6 is selected for the AES, RSA Security will *not* require any licensing or royalty payments for products using the algorithm".

The emphasis on the word "if" suggests that RSA Security Inc. may have required licensing and royalty payments for any products using the RC6 algorithm. RC6 was a patented encryption algorithm (U.S. Patent 5,724,428 (https://www.google.com/patents/US5724428) and U.S. Patent 5,835,600 (https://www.google.com/patents/US5835600)); however, the patents expired between 2015 and 2017.

Notes

- Pavan, R.L.; Robshaw, M.J.B.; Sidney, R.; Yin., Y.L. (1998-08-20). "The RC6 Block Cipher" (http://people.csail.mit.edu/rivest/pubs/RRSY98.pdf) (PDF). v1.1. Retrieved 2015-08-02.
- Beuchat, Jean-Luc. "FPGA Implementations of the RC6 Block Cipher" (https://web.archive.org/web/20060505225326/http://perso.ens-lyon.fr/jean-luc.beuchat/Publications/fpl2003.pdf) (PDF).

Archived from the original (http://perso.ens-lyon.fr/jean-luc.beuchat/Publications/fpl2003.pdf) (PDF) on 2006-05-05.

- Thompson, Iain (2013-12-31). "How the NSA hacks PCs, phones, routers, hard disks 'at speed of light': Spy tech catalog leaks" (https://www.theregister.co.uk/2013/12/31/nsa_weapons_catalogue_promises_pwnage_at_the_speed_of_light/). *The Register*. Retrieved 2015-08-02.

References

1. Hoang, Viet Tung; Rogaway, Phillip (2010). "On Generalized Feistel Networks". *LNCS 6223*. CRYPTO 2010. USA: Springer. pp. 613–630. doi:10.1007/978-3-642-14623-7_33 (https://doi.org/10.1007%2F978-3-642-14623-7_33).
2. "Confirmed: hacking tool leak came from "omnipotent" NSA-tied group" (https://arstechnica.com/security/2016/08/code-dumped-online-came-from-omnipotent-nsa-tied-hacking-group/). *Ars Technica*. August 16, 2016.
3. "These instructions guide the INSTALLATION of BLATSTING using ELIGIBLEBACHELOR via NOPEN tunnel" (https://github.com/nneonneo/eqgrp-free-file/blob/master/Firewall/BLATSTING/BLATSTING_20322/opinstructions/install.txt). Retrieved 2016-08-16.
4. "3.6.4 What are RC5 and RC6?" (https://www.emc.com/emc-plus/rsa-labs/standards-initiatives/rc5-and-rc6.htm). RSA Laboratories. Retrieved 2015-08-02.

External links

- "Cryptography - 256 bit Ciphers: Reference source code and submissions to international cryptographic designs contests" (http://embeddedsw.net/Cipher_Reference_Home.html#RC6).
- "Symmetric Ciphers: RC6" (http://www.users.zetnet.co.uk/hopwood/crypto/scan/cs.html#RC6). Standard Cryptographic Algorithm Naming (SCAN). 2009-04-15.
- "RC6® Block Cipher" (https://www.emc.com/emc-plus/rsa-labs/historical/rc6-block-cipher.htm). RSA Laboratories.
