RC5

From Wikipedia, the free encyclopedia

In cryptography, **RC5** is a block cipher notable for its simplicity. Designed by Ronald Rivest in 1994,[2] *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.

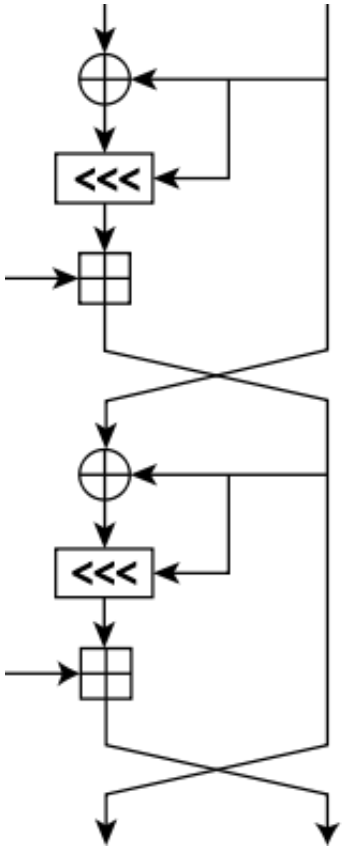
Contents

Description

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 choice 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 tantalising 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.

RC5



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

General

Designers	Ron Rivest
First published	1994
Successors	RC6, Akelarre

Cipher detail

Key sizes	0 to 2040 bits (128 suggested)
Block sizes	32, 64 or 128 bits (64 suggested)
Structure	Feistel-like network
Rounds	1-255 (12 suggested originally)

Best public cryptanalysis

12-round RC5 (with 64-bit blocks) is susceptible to a differential attack using 2^{44} chosen plaintexts.[1]

Cryptanalysis

12-round RC5 (with 64-bit blocks) is susceptible to a differential attack using 2^{44} chosen plaintexts.[1] 18–20 rounds are suggested as sufficient protection.

RSA Security, which has a patent on the algorithm,[3] offered a series of US$10,000 prizes for breaking ciphertexts encrypted with RC5, but these contests have been discontinued as of May 2007. A number of these challenge problems have been tackled using distributed computing, organised by Distributed.net. Distributed.net has brute-forced RC5 messages encrypted with 56-bit and 64-bit keys, and is working on cracking a 72-bit key; as of December 2012, 2.671% of the keyspace has been searched. At the current rate, it will take approximately 120 years to test every possible remaining key, and thus guarantee completion of the project.[4]

See also

- Madryga
- Red Pike

References

1. ^ ***a*** ***b*** Biryukov A. and Kushilevitz E. (1998). Improved Cryptanalysis of RC5. EUROCRYPT 1998.
2. ^ Rivest, R. L. (1994). "The RC5 Encryption Algorithm" (http://theory.lcs.mit.edu/~rivest/Rivest-rc5rev.pdf) (pdf). *Proceedings of the Second International Workshop on Fast Software Encryption (FSE) 1994e*. pp. 86–96.
3. ^ Rivest, R. L, "Block Encryption Algorithm With Data Dependent Rotation", U.S. Patent 5,724,428 (http://www.google.com/patents/US5724428), issued on 3 March 1998.
4. ^ [1] (http://stats.distributed.net/projects.php?project_id=8)

External links

- Rivest's paper describing the cipher (http://people.csail.mit.edu/rivest/Rivest-rc5.pdf)
- SCAN's entry for the cipher (http://www.users.zetnet.co.uk/hopwood/crypto/scan/cs.html#RC5)
- RSA Laboratories FAQ — What are RC5 and RC6? (http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/rc5-and-rc6.htm)
- Helger Lipmaa's links on RC5 (http://research.cyber.ee/~lipmaa/crypto/link/block/rc5.php)

Categories: Block ciphers | Broken block ciphers
