TECHNICAL SCIENCES

APPLICATION OF CAST-256 IN A LOGICAL TASKS

Akhmetova A.
Department "Artificial Intelligence and BigData " PhD
Kazakh National University al- Farabi
Maksutova Sh.
teacher of Department "Information systems"
Kazakh National University al- Farabi
Toktassyn A.
master of Department "Artificial Intelligence and BigData"
Kazakh National University al- Farabi
Bazarbek Zh.
master of Department "Informatics"
Kazakh National University al- Farabi
Ilessova B.
master of Department "Information systems"
Kazakh National University al- Farabi

Abstract

The article contains the algorithm of the cryptographic system CAST-256. The article provides a brief explanation and structure of block ciphers. The task of the CAST-256 cryptographic system is performed according to the algorithm and was calculated manually. The task performed by the CAST-256 cipher is solved by transformations.

Keywords: cryptography, encryption, block cipher, algorithm, cast -128, cast-256, cryptanalysis, logical task.

Cryptography concepts. The use of cryptography in modern digital technologies is becoming an integral part of many areas of our society. This process is becoming more and more large-scale. More and more often in our everyday life there are such concepts as login and password, authentication and identification, electronic digital signature, public and private key encryption, and many others.

The concept of "security" covers a wide range of interests, both of individuals and of entire states. In all historical times, significant attention was paid to the problem of information security, to ensure the protection of confidential information from acquaintance with competing groups. It's not without reason that the great psychologist William Shakespeare in the King Lear said: "Let the hearts open, and not that letters, in order to recognize the enemy's thought." There were three main ways to protect information. The first method involved purely forceful methods: protection of a document (information carrier) by individuals, its transfer by a special courier, etc [1,2].

The second method was called "steganography" and consisted in hiding the very fact of the availability of classified information. In this case, in particular, the so-called "sympathetic inks" were used. With appropriate manifestation, the text became visible. One of the original examples of information hiding is given in the works of the ancient Greek historian Herodotus. On the head of a slave who was shaving her head, the desired message was recorded. And when his hair grew enough, the slave was sent to the addressee, who again shaved his head and read the received message. The idea of exotic protection of secret texts (including the use of sympathetic inks) has survived to the present day.

The third way to protect information was to convert the semantic text into a chaotic set of characters (letters of the alphabet). The reporting recipient was able to convert it to the original meaningful message, if possessed the "key" to its construction. This method of protecting information is called cryptographic. According to some experts, cryptography by age is the same age as the Egyptian pyramids [5].

Cast-256 Algorithm Specification. The CAST-256 encryption algorithm was developed by specialists from the Canadian company Entrust Technologies. The basis of the algorithm is the conversion of the widely used and well-proven CAST-128 algorithm, also developed by Entrust Technologies.

The CAST-256 algorithm encrypts information with 128-bit blocks and uses several fixed sizes of the encryption key: 128, 160, 192, 224 or 256 bits.

A 128-bit data block is divided into 4 sub-blocks of 32 bits, each of which in each round of the algorithm undergoes a certain transformation and is superimposed on one of the neighboring sub-blocks. The developers of the algorithm classified it as a permutation-permutation network [10]. However, a number of experts at the AES competition considered the CAST-256 algorithm as the Feistel network, in each round of which only one sub-block is processed, and the number of "real" rounds is 4 times more than stated in the specification of the algorithm [6].

During the operation of the algorithm, 12 rounds of transformations are performed, in the first 6 of which the *tl* transform (called the direct function of the round) is performed, and in the last 6 rounds the inverse round function *tl* is performed. The *tl* function is described as follows:

$$C = C \oplus f1(D, Kr_{0l}, Km_{0l});$$

$$B = B \oplus f2(C, Kr_{1i}, Km_{1i});$$
$$A = A \oplus f3(B, Kr_{2i}, Km_{2i}); \quad (1)$$
$$D = D \oplus f1(A, Kr_{3i}, Km_{3i});$$

i - is the number of the current round.

The ti conversion consists of the following operations:

$$D = D \oplus f1(A, Kr_{3i}, Km_{3i});$$
$$A = A \oplus f3(B, Kr_{2i}, Km_{2i}); \quad (2)$$
$$B = B \oplus f2(C, Kr_{1i}, Km_{1i});$$
$$C = C \oplus f1(D, Kr_{0i}, Km_{0i});$$

Functions perform several elementary operations on a 32-bit subunit; they are shown, respectively, in figure 3. Each function takes three parameters:

- value of the processed subunit (indicated in the figures as "data");
- 32-bit subkey of the Km_{ni} round (called a masking subkey, since the first operation of each function is to overlay this key on the processed sub-block);
- 5-bit subkey of the Kr_{ni} round (called a shift subkey, since this key is used in the cyclic shift operation of the result of the previous operation by a variable number of bits) [14].

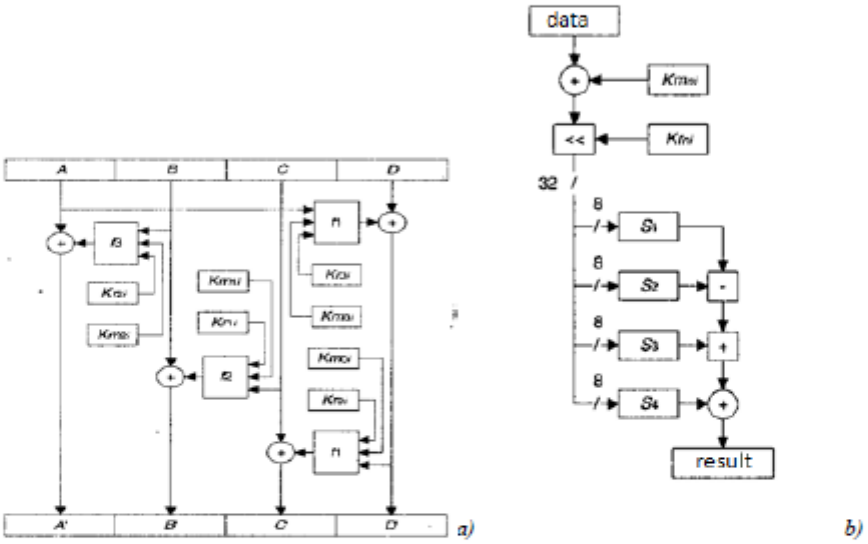

Figure 1. Transformations

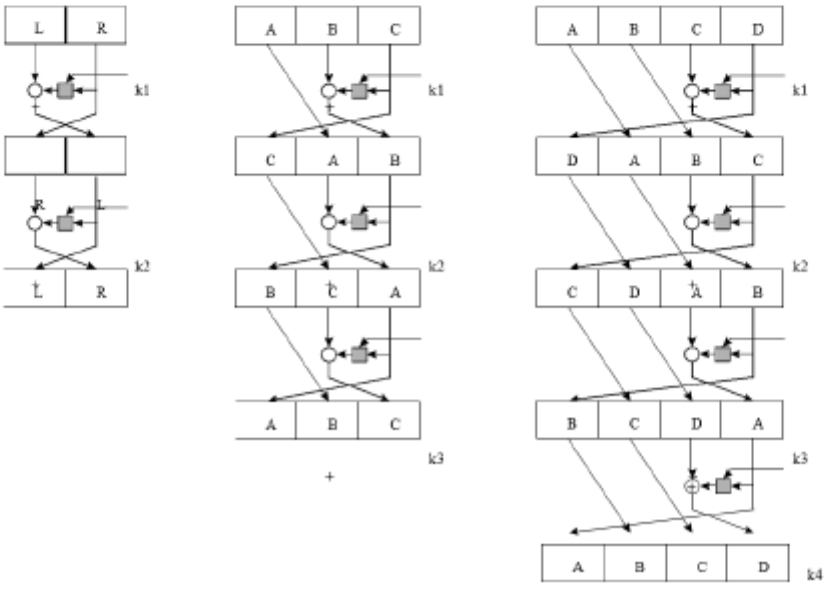

Figure 2. Algorithm clarification

Task solution. Research results.

1-round characteristic. Describe the characteristic

$$(0,0,\beta,\alpha) \xrightarrow{1roundA^2(p=2^{-17})} (\alpha,0,0,0).$$

Consider the function F2 and assume that Kr is abstract. If u1⊕u2=29$_x$<<<24-Kr.

The difference of this pair after bitwise addition with Km is preserved, v1⊕v2=29$_x$<<<24-Kr. After turning on the Kr bit the difference becomes equal 29$_x$<<<24. So the input difference on S1 equal 29$_x$, and all the others S-boxes have zero input (so and output) difference, that is $v_1[23,\dots,0] = v_2[23,\dots,0]$. So let's put $z{:=}S_3(v_1[15,\dots,8]) - S_2(v_2[23,\dots,16]) = S_3(v_2[15,\dots,8]) - S_2(v_2[23,\dots,16])$, then we can write:

$$W_1 := (S_1(v_i[31,\dots,24]) + z) \oplus S_4(v_1[7,\dots,0]), i = 1,2$$

Search of all possible 256 input pairs in S1 showed that two of them with a difference of 29$_x$: (17x, 3Ex) and (3Ex, 17x) provide an input difference. Considering this case, that is when $(S_1(v_1[31,\dots,24]) + z) \oplus S_1(v_2[31,\dots,24]) + z)$, we receive β with probability 2^{-5}, because Hamming's weight β is 5:

$$(S_1(v_1[31,\dots,24]) + z) \oplus S_1(v_2[31,\dots,24]) + z) = \beta$$

Bitwise addition with output S_4 does not change difference.

So that, assuming that the value of Kr is known, the input difference 29$_x$<<<24-Kr leads to the output difference β with probability 2^{-12}. Because Kr is not known, we can guess it by noticing that α equals 29$_x$<<<24 with probability 2^{-5} and output difference F^2 function equals β with probability 2^{-17}.

Let's pay attention to a round of type A2 with input difference $(0,0,\beta,\alpha)$. Output difference F2 function, equal β, bitwise is added to the third word by input difference round A2, and it turns out zero.

2-round and 15-round characteristic.

This characteristic $(\beta,\alpha,0,0,) \xrightarrow{2roundA(p=1)} (0,0,\beta,\alpha)$ and the characteristic which presented in the *table 1* obviously follows the structure of the rounds of the CAST -256 cipher.

Table 1.

15-round characteristic with probability 1

	3-round A	12-round B
α	0 0 0	0 0 α 0 0 0 α 0 0 α
0	α 0 0	0 0 0 0 0 α 0 0 0 α 0 0
0	0 α 0	α 0 0 α 0 a 0 0 0 a
0	0 0 α	0 0 a 0 0 0 a

At the beginning, the plaintext is converted by 24-rounds of type A and then 24-rounds of type B, the exact sequence of rounds is as follows:

$$A^1A^2A^3, A^1, A^1, A^2, A^3, A^1, A^1, A^2, A^3, A^1, \dots$$
$$B^1, B^2, B^3, B^1, B^1, B^2, B^3, B^1, B^1, B^2, B^3, B^1, \dots$$

Consider the example of manual calculation of the first round of encryption and decryption of text.

$$s_1 = 1011101, s_2 = 10111000, s_3 = 10111101, s_4 = 10101101$$
$$k_m = 1101111011, k_r = 11011011, k_{rl} = 5 \text{ small bit}, k = 101101101, k_r = 11011$$
$$k{=}K_r 11011 \oplus S_1 10101101 = 1111010100 \rightarrow -C8 + 89FE78E6$$
$$= 89FE79AE \oplus 0D23E0F9 = 84DD9957 - 68458425$$
$$= 1C981532 + 56C8C391 = 7360D8C$$
$$B = 10111101 \oplus 11011 = 10100110 = A6 + S_1 + 5608c391$$
$$= 56c8c437 - s_2 d23e0f9 = 049a4e33e + s_3 68458425$$
$$= b1ea6763 \oplus s_4 56c8c391 = e722a4f2$$
$$C = 10111000 - 110111 = 10000001 = 1 + S_1 56C8C391$$
$$= 56C8C412 + S_2 0D23E0F = 63ECA50D \oplus S_3 68458425C$$
$$= 6E7D4E757 - S_4 56C8C391 = 690EC23C6$$
$$D = 10000001 \oplus S_1 10101101 = 100101100$$
$$D' = 100101100 - 110101101 = 10000001$$
$$C' = 690EC23C6 + 56C8C391 = 6E7B4E757 \ominus 68458425$$
$$= 63E6CA50B - 56C8C412 - 56C8C391 = 81 \rightarrow q_2$$
$$= 10000001 + 110111 = 10111000$$
$$B' = E722A4F2 \ominus 56C8C391 = B1EA6763 - 68458425 = 49A4E33E + d23e0f9$$
$$= 56c8c437 - 56c8c391 = A6$$
$$A' = 7360D8C3 - 56C8C391 = 1C981532 + 68458425 = 84dd9957 \ominus d23e0f9$$
$$= 89ffe79ae - 89fe78e6 = c8$$

The article describes a differential attack on the CAST -256 cipher, which is more effective than previously known attacks on this cipher. This attack is based on a truncated differential characterization covering 18 rounds of cipher.

References

1. Alferov A.P., Zubov A.Yu., Kuzmin A.S., Cheremushkin A.V. Basics of cryptography.

2. Menezes, P. van Oorschot, S. Vanstone Handbook of Applied Cryptography. – CRC Press, Inc. – 1997.

3. Petrov A.A. Computer security. Cryptographic methods of protection. M.: LITE Ltd., 2002.

4. C. Adams, "Simple and Effective Key Scheduling for Symmetric Ciphers", in Workshop Record of the Workshop on Selected Areas in Cryptography (SAC '94), Kingston, Canada, May 1994, pp.129-133.

5. H. Feistel, "Cryptography and Computer Privacy", Scientific American, vol. 228, no. 5, 1973, pp.15-23.

6. S. Moriai, T. Shimoyama, and T. Kaneko, "Higher Order Differential Attack of a CAST Cipher", Proceedings of the Fifth International Workshop on Fast Software Encryption, Paris, France, March 1998, LNCS 1372, Springer, pp.17- 31.

7. Grusho A.A., Primenko E.A., Timonina E.E. Analysis and synthesis of cryptographic algorithms. Lecture course. Moscow 2000.

8. Dadukov, N.S. Soviet encryption technology [Text]: Leningrad period: 1935-1941 / N. S. Dadukov [et al.] // Information Security. Insider. - 2006. - N 1. - pp. 91-96. - 2006.

9. Donald E. Knut Chapter 3. Random numbers // The Art of Programming. - 3rd ed. - M.: Williams, 2000. - T. 2. The resulting algorithms. – p. 832 .

10. https://www.researchgate.net/publication/3608347_On_the_security_of_the_CAST_encryption_algorithm

11. https://tools.ietf.org/html/rfc2612

12. Advanced Encryption Standard (AES) project. 1997-2000. URL: http//esre.nist.gov/encryption/aes.

13. Schneier B.A Self-study course in block-chipher cryptoanalysis//Cryptologia.2000. №1.P.18-34.

14. Adams C. The CAST-256 Encryption Algorithm. AES submission. – 1998. URL: www.networkdls.com/Articles/cast-256.pdf.

15. Wagner D. The boomerang Attack//Proc. of Fast Software Encryption'99. Future Notes in Computer Science. Springer-Verlag.1999. Vol. 1636.P.156-170.

16. Seki H., Kaneko T. Differential Cryptanalysis of CAST -256 Reduced to Nine-Rounds//IEICE Trans. Fundam. Electron. Commun. Comput. Sci. 2001.Vol.E84-A №913-918

17. Biham E., Shamir A. Differential Cryptanalysis of DES-like cryptosystems.-1991. Vol.4.P.3-72.