УДК 004.056.55

# *ПРОГРАММНАЯ РЕАЛИЗАЦИЯ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ С ПОМОЩЬЮ АЛГОРИТМА 2DES*

***Головченко О. Н.***

*магистрант*

*Южно-Российский государственный политехнический университет (НПИ)*

*имени М.И. Платова*

*Новочеркасск, Россия*

***Оганян Р. Г.***

*аспирант*

*Южно-Российский государственный политехнический университет (НПИ)*

*имени М.И. Платова*

*Новочеркасск, Россия*

**Аннотация.**

В данной статье осуществлена программная реализация криптографической защиты с помощью алгоритма 2des. Описывается алгоритм 2des.

**Ключевые слова:** криптографическая защита, программная реализация, алгоритм 2des.

# *SOFTWARE IMPLEMENTATION OF CRYPTOGRAPHIC PROTECTION BY MEANS OF 2DES ALGORITHM*

***Golovchenko O.N.***

*master student*

*South-Russian State Polytechnic University (NPI)*

*Novocherkassk, Russia*

***Oganyan R.G.***
*graduate student*
*South-Russian State Polytechnic University (NPI)*
*Novocherkassk, Russia*

**Abstract**
This article has implemented software implementation of cryptographic protection using the 2des algorithm. The 2des algorithm is described.
**Key words:** cryptographic protection, software implementation, algorithm 2des.

One of the most well-known cryptographic systems with a private key is DES - Data Encryption Standard. This system was the first to receive the status of a state standard for data encryption. It was developed by IBM specialists and took effect in the USA in 1977. The DES algorithm was widely used in storing and transferring data between different computing systems; in postal systems, in electronic systems of drawings and in the electronic exchange of commercial information. The DES standard was implemented both in software and hardware. Enterprises of different countries have launched a mass production of digital devices using DES for data encryption. All devices are subject to mandatory certification for compliance with the standard [1,2].

The process of encrypting each 64-bit block of source data can be divided into three stages:

-initial preparation of the data block;

-16 rounds of the "main cycle";

-final processing of the data block.

At the first stage, an initial permutation of the 64-bit source text block is performed, during which the bits are reordered in a certain way.

At the next (main) stage, the block is divided into two parts (branches) of 32 bits each. The right branch is transformed using a certain function F and the corresponding partial key obtained from the main encryption key using a special key conversion

algorithm. Then the data is exchanged between the left and right branches of the block. This is repeated in a loop 16 times.

Finally, in the third stage, the result is rearranged after sixteen steps of the main loop. This permutation is the inverse of the initial permutation.

To increase DES cryptographic strength, several options appear: double DES (2DES), triple DES (3DES), DESX, G-DES.

The 2DES and 3DES methods are based on DES, but they increase the length of the keys (2DES — 112 bits, 3DES — 168 bits), and therefore the robustness increases.

Encrypted three times with 3 different keys.

DES-EDE3: 3DES operations encryption-decryption-encryption with 3 different keys.DES-EEE2 and DES-EDE2: Like previous ones, except that the first and third operations use the same key [3].

Two-time DES is also called 2DES.

Encryption: C = Ek2 (Ek1 (P)).

Decryption: P = Dk1 (Dk2 (C)).

In case of a full brute-force attack, 22n attempts (encryption) will be needed, where n is the key length. But Merkle and Hellman offered a special “meeting in the middle” attack for hacking 2DES, which requires 2n + 1 encryption. In this attack, encryption is performed on one side, decryption on the other, and the results obtained in the middle are compared. In this attack, the cryptanalyst knows pairs of 2 “plaintext-ciphertext” P1, C1 and P2, C2 such that

C1 = Ek2 (Ek1 (P1)), C2 = Ek2 (Ek1 (P2)). It is necessary:

1. For each key k, calculate Ek1 (P1) and store the results in memory.

2. For each key k, calculate Dk (C1) and find the same result in memory.

3. If such a result is found in memory, then the current key is probably k2, and the key for the result in memory is k1.

4. Execute text encryption using 2DES; if C2 is obtained, then the keys are found correctly. If not, continue searching. But an attack requires a large amount of memory - 56 2 64-bit blocks, which is 17 ≈10 bytes [4].

Software implementation of this algorithm is given below. First you need to enter a message that you want to encrypt (Figure 1).

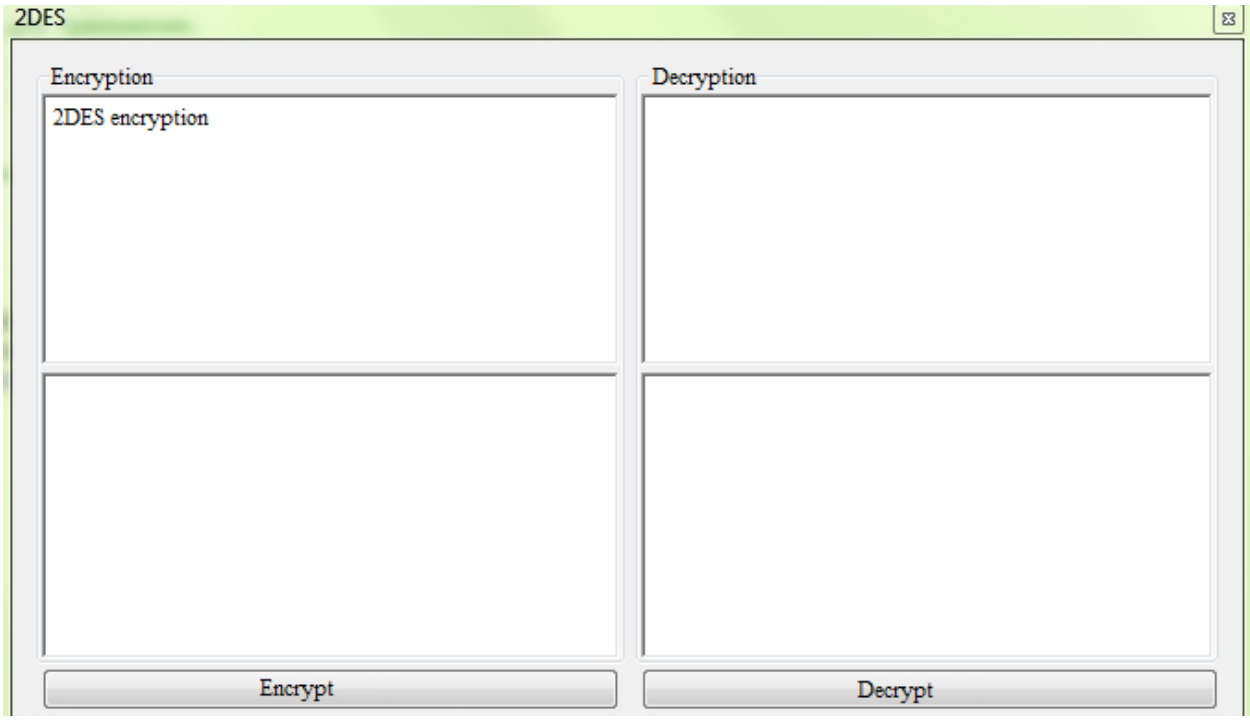


Fig.1 - Entering the word to be encrypted

After entering the message, you must click on the “Encrypt” button. The result is shown in Figure 2.

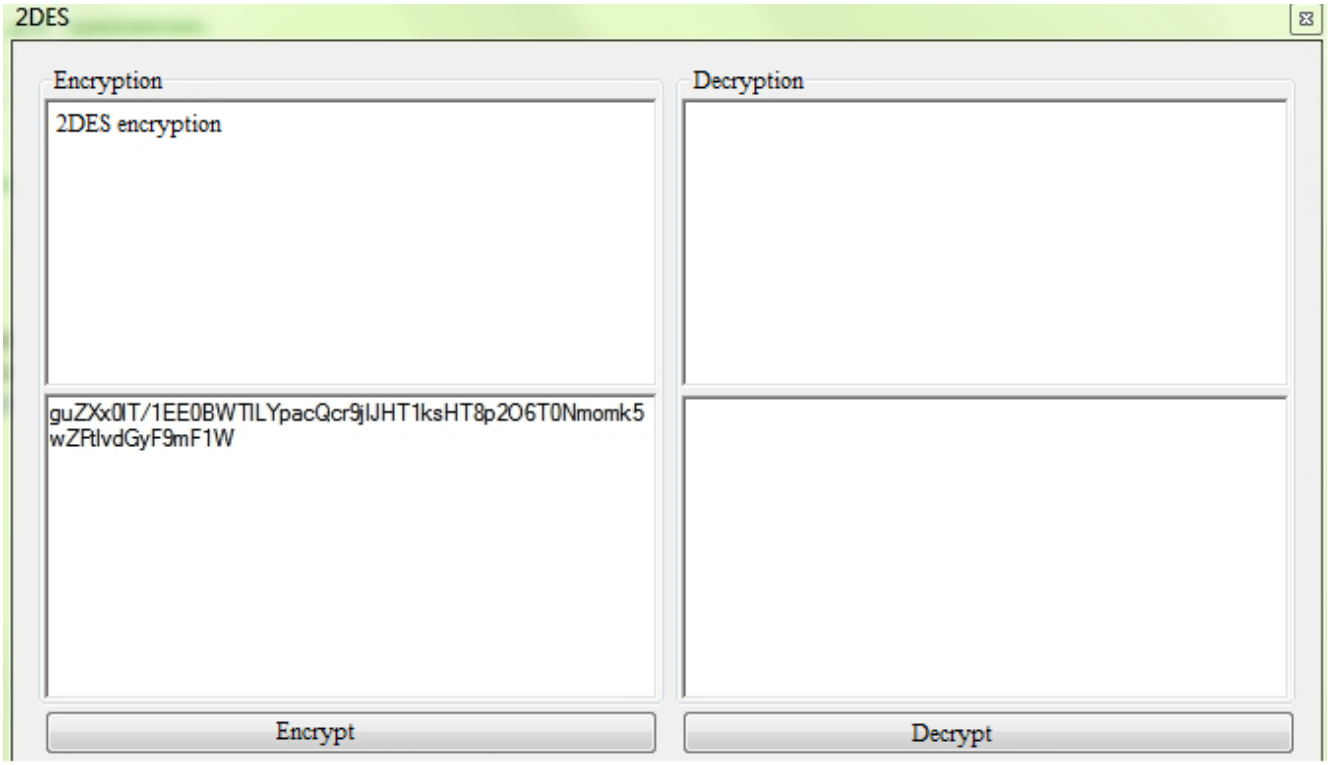


Fig.2 - Getting encrypted text

To decrypt this message, copy the encrypted text and paste it into the adjacent window, as shown in Figure 3.

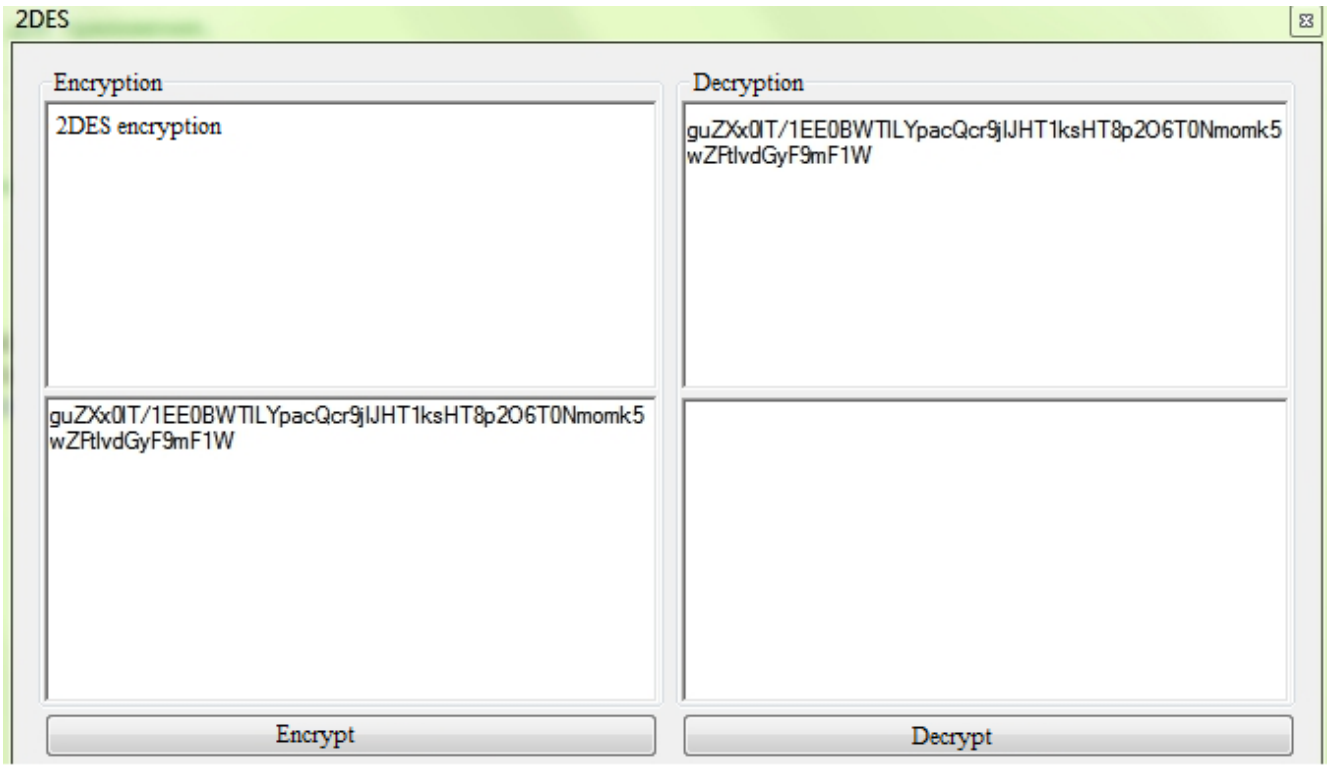


Fig.3 - Entering encrypted text

Next, you need to click on the “Decrypt” button, as a result of which the original message will be displayed (Figure 4).

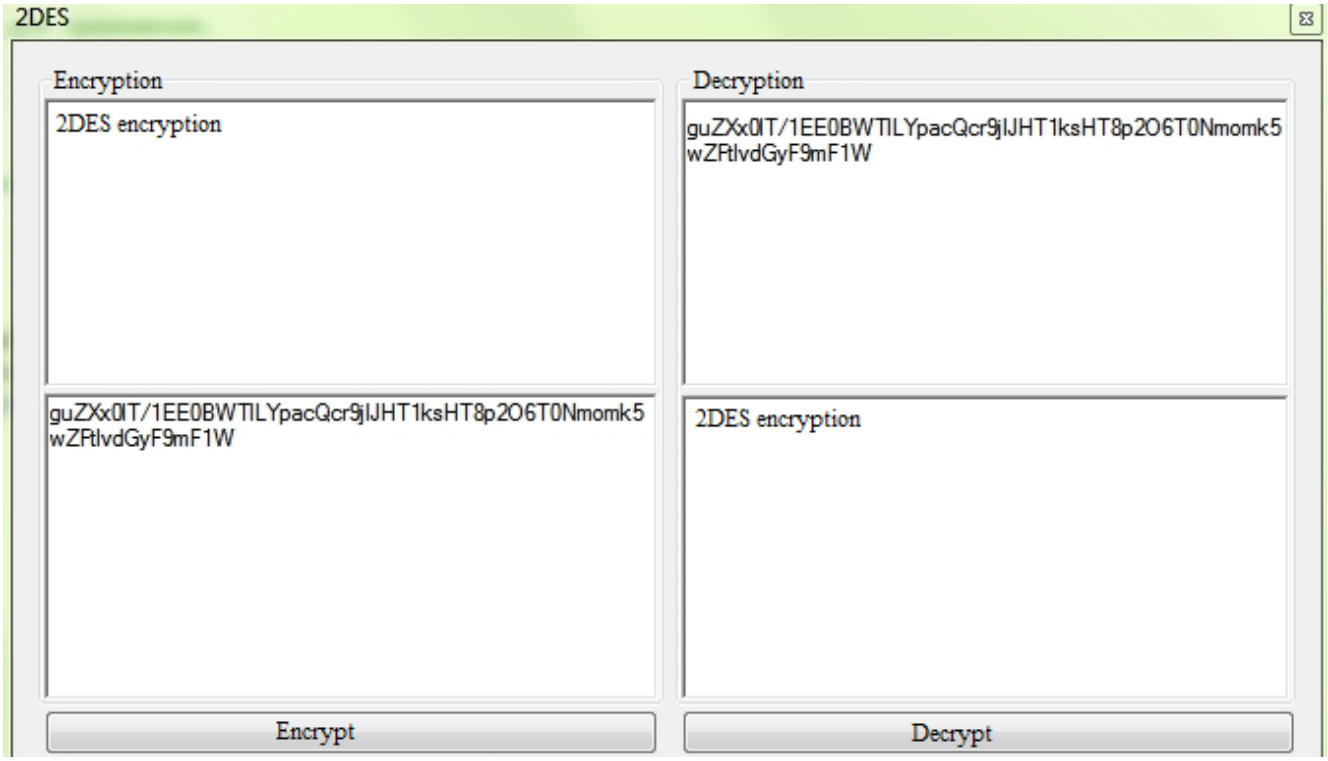


Fig.4 - Reception of decoded text

Thus, the 2des algorithm was described, and the software development of the application was organized using this method. This message encryption provides additional security.

**References :**

1. DES and AES encryption algorithms [Electronic resource]. - Access mode: https://www.intuit.ru/studies/courses/691/547/lecture/12377 (circulation date 01.02.2019).

2. DES [Electronic resource]. - Access mode: http://kriptografea.narod.ru/DES.html (circulation date 01.02.2019).

3. DES (Data Encryption Standard) [Electronic resource]. - Access mode: https://ru.bmstu.wiki/DES_(Data_Encryption_Standard) (circulation date 01.02.2019).

4. DES algorithm [Electronic resource]. - Access mode: https://www.opennet.ru/docs/RUS/inet_book/6/des_641.html (circulation date 16.01.2019).

*Оригинальность 90%*