УДК 004.7

DEVELOPMENT OF A DIGITAL ENCRYPTION PROGRAM AND IMPLEMENTATION IN PRACTICE

Qodirov Farrux Ergash o'g'li 4th year student

Karshi branch of the Tashkent University of Information Technologies named after Muhammad al-Khorezmi

Annotation: It is noteworthy that the 21st century was the century of information technology. The emergence of digital integrated circuits allowed us to control devices using software. In addition, the advent of the discovery of the optical communication system and the discovery of similar technologies have become one of the urgent problems in ensuring the data transmission, processing and security of information technologies and telecommunication systems. What we are doing in this respect is commendable. Definitely cryptographic! At present, the "information concept" is often used as a private trademark, which can be bought, sold, or replaced with another.

Keywords: Cryptographic, cybercriminals, encryption, algorithm unauthorized.

At the same time, the value of information is often multiplied several hundred thousand times by the cost of its embedded computer system. Therefore, it is quite natural that there is an urgent need for access to information, without going into it, deliberately changing, stealing, losing it and avoiding other types of criminal trafficking.

Under the protection of information in computer systems and networks refers to the use of various tools and measures to ensure the systematic reliability of the stored, stored and processed information.

Let's look at some encryption methods. There are two modifications for coding the value of the downloaded information: encoding and encryption.

Books or tables containing a set of frequently used expressions are used for encoding. Each of these terms has an optional coded word, often in a set of numbers. Encoding information requires a similar book or table. A coding book or table is an example of an optional cryptographic replacement. Compliance

information technology coding - converting lane data into numerical data and making opposite changes. The encryption book can be run on both fast and external storage devices, but such a fast and reliable cryptographic system is not successful. If you use this book without permission, you will need to create a new code and distribute it to all users.

The second type of cryptographic modification does not include encryption, which includes formatting algorithms that cannot be captured by the initial text characters. This type of change is consistent with information and communication technology. Here it is important to protect the algorithm. Using a cryptographic key, you can reduce the security requirements in the encryption algorithm itself. Now the object of protection is only the key to quality. If the key has been copied, you can change it, and this is easier than changing the book or table. Therefore, encryption is not encryption, but is widely used in information and communication technologies.

Currently, information technology is protected by a variety of coding methods and software. No one can deny that attacks on these systems were made by promiscuous and professional hackers. Today, all security systems, encryption algorithms and encryption methods are widely used. At the moment, these systems have proven to be difficult for Cyberspace. This is based on the Tass.ru website, which is based on statistical information published under the heading "Hacker attacks in 2001-2016" (June 1, 2016). For example: in April 2009, cybercriminals penetrated the Pentagon’s computer system and stole information about a new generation of fifth-generation combat fighter.

- On July 7, 2009, hackers closed almost all of South Korea’s main internet portals, including the websites of the president, parliament and defense ministries.

- In June 2011, Citigroup (USA), a banking conglomerate, reported approximately 360,000 streams of personal data as a result of an unidentified hacker attack.

- On July 21, 2011, the Anonymous hacker group attacked government sites and sites of large companies from different countries and announced the destruction of the NATO base.

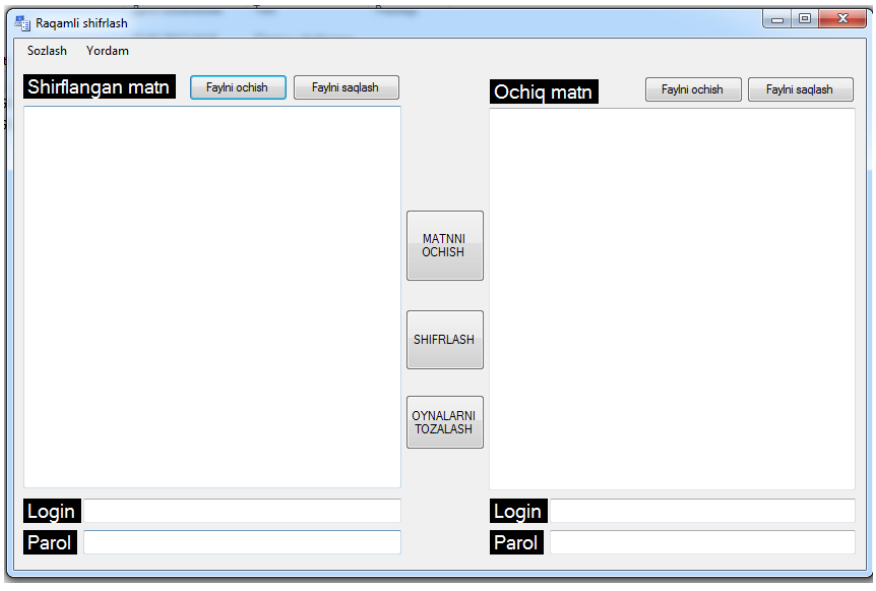
- On February 10, 2016, the official tax administration of Japan and the Japanese Foreign Trade Organization (JETRO) were eliminated as a result of DDoS attacks. Responsibility for this is borne by anonymous international hackers.

This statistic can be resumed again. Cause! very simple, but also all currently used systems of security, coding, encryption methods, and all software running on mathematical, logical operations. At the same time, security systems are also wary of “cybercriminals”.

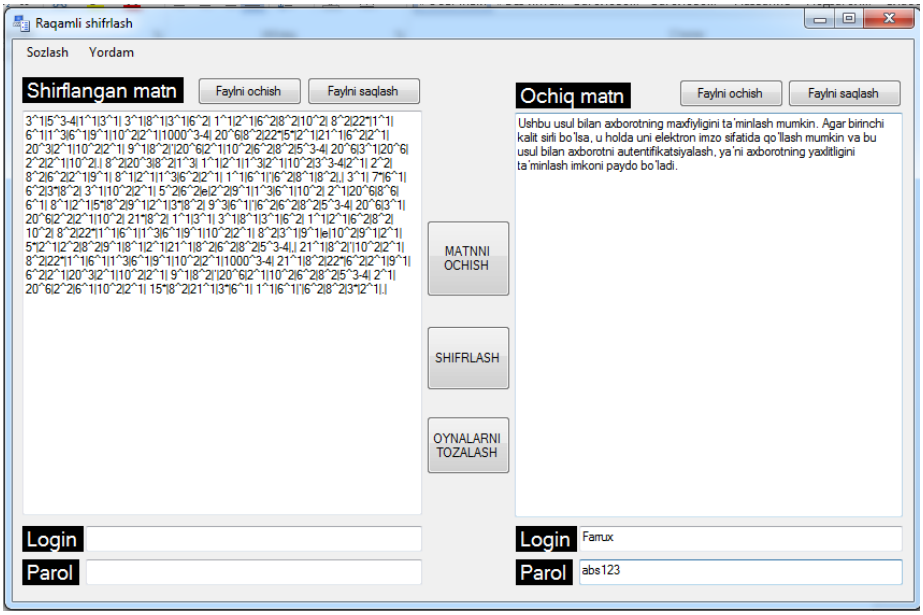
Shakhasanov is not a new mathematical, logical thing for world scientists and programmers! Without serial codes! You can not ignore it! Without the use of secure systems of protection and encryption methods, it is necessary to propose a new method that is used in all areas.

In April 2017, the idea of creating new cryptographic software was born. In a short time, an encryption algorithm was developed and an algorithm was developed.

This method can ensure the confidentiality of information. If the first key is mysterious, then it can be used as an electronic signature, which allows you to authenticate information, that is, the integrity of information.



Pic.1 Digital encryption software interface (general form).



Pic.2 Text is encrypted.

This coding method is based on the use of letters and numbers in the usual Uzbek Latin alphabet, in which multiplication, division, multiplication, addition, substitution are not performed. This encryption method is very simple. It is enough to know the 29 letters of the Latin alphabet. The program is based on letters and numbers. Considering that there are several common alphabets in the world, this program may be different in all countries.

This software is based on a new encryption algorithm. As mentioned above, the principle of operation can be in a simple, but new and complex way. The advantage of the program is that unauthorized methods and algorithms were used, and the process of program authentication and authentication was also considered. The ability to use audio, video, animation and data transmission in the telecommunications network for transmission, reception and encoding. may also occur.Pic.2 Text is encrypted.

The program can work only in the Latin alphabet, except for W and C. The biggest drawback is the ability to encode a text file. There are currently no methods for encoding audio and video, characters and foreign alphabets (languages). Another minor drawback of the program is that it does not access the office

software library for saving information in a file format (* .docx, * .docm, * .pdf, * .doc, * .dot, * .dotx,). (* .txt) libraries to open.

Using digital encryption, we were able to encode text information and analyzed the results. We are conducting a series of studies to further develop this program and continue to work on improving its civic potential. We will use the features of this digital encryption program in the future with a lot of work.

References:

1. Jel’nikov V. Kriptografiya ot papirusa do komp’yutera. M.: ABF, 1997. – 33
2. Nil’s Fergyuson, Bryus SHnayer «Prakticheskaya kriptografiya», M.: Izdatel’skiy dom «Vil’yams», 2005g.-424s.
3. Petrov A.A. «Komp’yuternaya bezopasnost’. Kriptograficheskie metodi zaщiti», M.: DMK, 2000g. -448s.
4. Koblits N. Kurs teorii chisel v kriptografii. – M., Nauchnoe izdatel’stvo TVP, 2001y.
5. akadmvd.uz/wp-content/.../2013-karimov-axborot-lat.pdf
6. library.ziyonet.uz/uz/book/download/34709