UDC 004.9 **doi: 10.26906/SUNZ.2024.1.050**

G. Golovko, O. Rudenko, A. Batrachenko, R. Kyzymenko

National University «Yuri Kondratyuk Poltava Polytechnic», Poltava, Ukraine

ORGANIZATION OF INFORMATION PROTECTION AT THE «DRIVE PETROL» ENTERPRISE USING A CRYPTOGRAPHIC ALGORITHM AES

Abstract. In today's digital age, information protection is becoming a dominant task, as the number of threats in the field of cyber security is constantly increasing. In this context, the implementation of effective protection means, among which encryption takes a key place, becomes especially important. The AES (Advanced Encryption Standard) cipher appears to be an exceptionally powerful tool aimed at ensuring data privacy. Information security is an extremely important aspect in the digital age, where cyber security threats are constantly increasing. In this context, encryption becomes a necessity, and the AES (Advanced Encryption Standard) cipher appears to be an exceptionally effective tool for ensuring data privacy. AES is used to protect information by converting it into cryptographically unreadable form. Due to the high degree of complexity and the possibility of using keys of different lengths, from 128 to 256 bits, AES guarantees a high level of security. Its resistance to attacks provides reliable protection against unauthorized access. One of the key advantages of AES is its versatility – it is used in a variety of industries, including finance, medicine, telecommunications, and more. The cipher has high performance, which makes it the optimal solution for protecting confidential information in a world where security becomes a priority. The application of AES not only protects data from unauthorized access, but also contributes to the overall level of security in the digital environment, ensuring excellent compatibility with various industries and user needs.

Keywords: cryptography, functions, cypher, aes, operator, algorithm.

Introduction

The problem of information protection is not new. It appeared long before the advent of computers. The rapid improvement of computer technologies also affected the principles of building information protection. From the very beginning of its development, information security systems were developed for military departments. Disclosure of such information could lead to huge casualties, including human casualties. Therefore, confidentiality (that is, non-disclosure of information) was given special attention in the first security systems. It is obvious that only their complete encryption can reliably protect messages and data from disclosure and interception. The main feature of the current situation is that the most important task today is the protection of information in computer networks [1].

The widespread introduction of computers in all types of activities, the constant increase in their computing power, the use of computer networks of various scales have led to the fact that the threat of loss of confidential information in data processing systems has become an integral part of almost any activity. The principle of modern information protection can be expressed as follows - the search for an optimal relationship between availability and security. A fully secured computer is one that is locked in an armored room in a safe, not connected to any network (not even electrical) and turned off. Such a computer has absolute protection, but it cannot be used. In this example, the requirement of availability of information is not fulfilled. The "absoluteness" of protection is hindered not only by the need to use protected data, but also by the complexity of protecting systems. [1]

Main part

1. Organization of information protection at the enterprise. An official - the head of the security department - is appointed to manage the means of information protection at the enterprise. His duties and competence:

- creation of a system of delimiting access and means of protection of the facility;
- protection of information from leakage through technical channels;
- implementation of technical measures for information protection.

2. Peculiarities of the implementation of the access demarcation system. In the access delimitation system, a dispatcher must be used, which performs access delimitation in accordance with the principle of delimitation.

Demarcation of access to information objects is carried out in accordance with the authorities of the subjects.

The basis of such demarcation is the selected access control model implemented by the access manager.

The manager ensures the implementation of the rules for demarcating the access of subjects to access objects, which are stored in the database of authorizations and access characteristics.

A request for subject access to some object is sent to the database management and event registration unit. The authority of the subject and the characteristics of the object are analyzed in the decision-making block. According to the results of the analysis, a signal of permission or refusal of permission is formed ("Allow", "Reject").

If the number of "Reject" signals exceeds a given level (for example, 5 times), which is fixed by the registration unit, then the decision-making unit signals "Unauthorized access".

Based on this signal, the security system administrator can block the subject's work to find out the cause of such violations.

Distribution of information is shown in Table 1.

Table 1 – **Distribution of information**

Departments \ Types of information	General information	Personal information	Financial information	Economic information	Legal information	Technical information
CEO	+	+	+	+	+	+
Accounting	+	-	+	-	-	-
Head of HR department	+	+	-	-	-	-
Chief designer	+	-	-	-	-	+
Level of confidentiality of information	N	N	S	S	S	R

N – not secret; S – secret; R – restricted

3. Information protection methods. Such a classification of information protection methods is usually considered:

1) legislative;
2) organizational;
3) technical;
4) software;
5) moral and ethical;
6) cryptographic [2].

The initial stage of the development of computer security is strongly connected with cryptography. The main conditions of information security are its availability and integrity. In other words, the user can at any time request the set of services he needs, and the security system must guarantee its correct operation. Any file or system resource, subject to compliance with access rights, should be available to the user at any time. If some resource is unavailable, then it is useless. Another task of protection is to ensure the immutability of information during its storage or transmission. This is the so-called integrity condition.

Performing encryption and decryption procedures, in any information process system, slows down data transfer and reduces their availability, because the user will wait too long for his "reliably protected" data, which is unacceptable in some modern computer systems. Therefore, the security system must first of all guarantee the availability and integrity of information, and then (if necessary) its confidentiality.

The AES cipher is a symmetric block encryption algorithm (block size 128 bits, key 128/192/256 bits), a finalist in the AES competition and adopted as the US encryption standard by the US government. The choice fell on AES with the expectation of widespread use and active analysis of the algorithm, as was the case with its predecessor, DES.

The US National Institute of Standards and Technology published the preliminary AES specification on October 26, 2001, after five years of preparation. On May 26, 2002, AES was announced as the encryption standard.

As of 2009, AES is one of the most widely used symmetric encryption algorithms [3].

4. Access restrictions. Demarcation of access is to provide each registered user with the opportunity to freely access information within the limits of his authority and to exclude the possibility of exceeding these authority. For each user, his authority regarding files and directories is established. [4]

The Bell-LaPadulla model is an access control and management model that is based on the mandated access control model (Tabl. 2).

Table 2 – **The Bell-LaPadulla model**

Departments \ Types of information	General information	Personal information	Financial information	Economic information	Legal information	Technical information
CEO	F	F	F	F	F	F
Accounting	R	N	F	N	N	N
Head of HR department	R	F	N	N	N	N
Chief designer	R	N	N	N	N	N

R – reading; N – no access; F – full access

The model analyzes the conditions under which the formation of information flows from subjects with a higher level of access to subjects with a lower level of access is impossible [4–6].

In the developed application, accounts were created for each user (Tabl. 3).

Table 3 – **Accounts for each user**

Office	Login (comp. name)	Password
State Department	deputydir	dpceo001
CEO	gendir	ceo001
Secretary	secret1	secret001
Secretary	secret2	secret002
Secretary	secret3	secret003
Chief Accountant	leadbuh2	leadbuh001

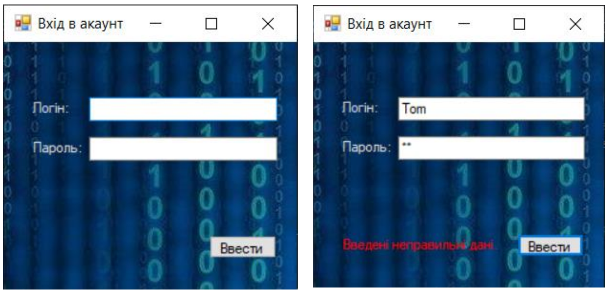
5. Presentation of the application/ After starting the program, we see the system login window (Fig. 1, a), if you do not enter the login and password, the program will not allow you to continue working (Fig. 1, b). Logging in is done using accounts for each user.

The menu window is shown in Fig. 2.

To work with the program, you need to create keys immediately (Fig. 3).

Then you can export these keys to your device for further work with them. In this case, when entering the program again, you will not have to create them again, you will only need to import them.

To encrypt a file, you need to click on "Encrypt file" (Fig. 4, 5). To decrypt the file, you need to click on "Decrypt file" (Fig. 6).



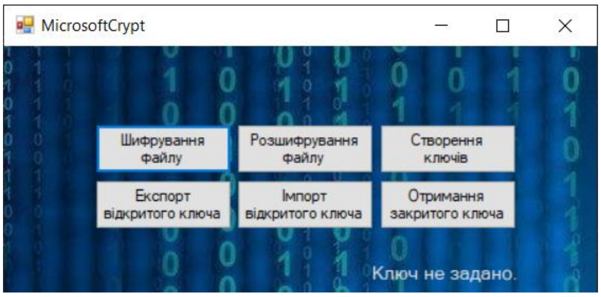
Tom

**

Введені неправильні дані

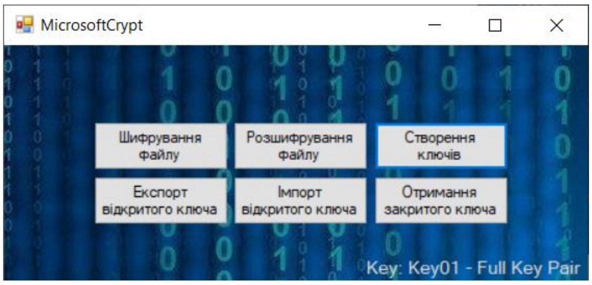
a b

Fig. 1. Login window



Ключ не задано.

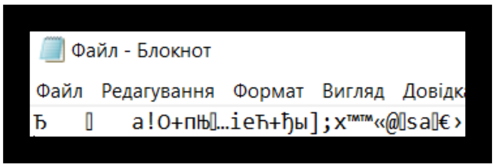
Fig. 2. Menu window



Key: Key01 - Full Key Pair

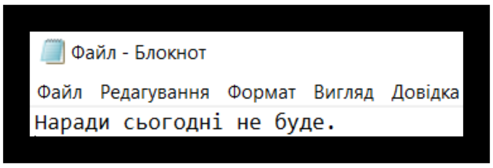
Fig. 3. An example of creating keys

Fig. 4. File for encryption



Ђ ▯ а!О+пњ▯…іеЋ+ђы];х™™«@▯sа▯€›

Fig. 5. File after encryption



Наради сьогодні не буде.

Fig. 6. File after decryption

Conclusion

As a result of the implementation of the scientific article, the project of organized means of information protection in the company "Drive Petrol" was developed. Demarcation of access was implemented, an access matrix and a mandated model of access to information were built. Information is also protected at the registry level and at the password level.

User accounts are created and an antivirus program is selected to protect the company's information from viruses, taking into account all the advantages and disadvantages.

An application has been developed, the main task of which is to encrypt data using the AES cipher.

References

1. Concept, essence, meaning of information protection. URL: http://www.infobezpeka.com/publications/?id=102.
2. Means of information protection. URL: https://stud.com.ua/94403/informatika/zasobi_zahistu_informatsiyi.
3. AES encryption. [Electronic resource]. – Access mode: http://kriptografea.narod.ru/AES.html.
4. Devyanin P.N. Safety models of computer systems: A textbook. Akademiya, 2005. P. 55-66.
5. Control, navigation and communication systems.
6. Golovko G., Matiashenko A., Solopihin N. Data encryption using XOR cipher.

Received (Надійшла) 29.11.2023
Accepted for publication (Прийнята до друку) 31.01.2024

Організація захисту інформації на підприємстві «Драйв Петрол» з використанням криптографічного алгоритму AES

Г. Головко, О. Руденко, А. Батраченко, Р. Кизименко

Анотація. В сучасному цифровому віці захист інформації стає домінуючим завданням, оскільки постійно зростає кількість загроз у сфері кібербезпеки. У цьому контексті особливо важливим стає впровадження ефективних засобів захисту, серед яких ключове місце займає шифрування. Шифратор AES (Advanced Encryption Standard) видається винятково потужним інструментом, спрямованим на забезпечення конфіденційності даних. Захист інформації – це надзвичайно важливий аспект у цифровому віці, де загрози кібербезпеки постійно зростають. У цьому контексті шифрування стає необхідністю, а шифратор AES (Advanced Encryption Standard) видається винятково ефективним інструментом для забезпечення конфіденційності даних. AES використовується для захисту інформації шляхом перетворення її у криптографічно нерозбірливий вигляд. Завдяки високій ступені складності та можливості використання ключів різної довжини, від 128 до 256 біт, AES гарантує високий рівень безпеки. Його стійкість до атак забезпечує надійний захист від несанкціонованого доступу. Однією з ключових переваг AES є його універсальність – він застосовується в різних галузях, включаючи фінанси, медицину, телекомунікації тощо. Шифратор володіє високою продуктивністю, що робить його оптимальним рішенням для захисту конфіденційної інформації у світі, де безпека стає пріоритетом. Застосування AES не лише забезпечує захист даних від несанкціонованого доступу, але й сприяє підвищенню загального рівня безпеки в цифровому середовищі, забезпечуючи відмінну сумісність із різними індустріальними галузями та потребами користувачів.

Ключові слова: криптографія, функції, шифр, aes, оператор, алгоритм.