УДК 004.7 **doi: 10.26906/SUNZ.2022.4.071**

G. Golovko, M. Tolochyn

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

USING THE AES ENCRYPTION METHOD IN PRACTICE

Abstract. Analysis of recent research and publications shows that Encryption methods vary by how much data they can handle at once and what kind of key it needs for its decryption. Some encryption is more easily hacked than others. While some companies or individuals choose encryption type according to standards dictated by legal or industrial regulations, others may simply choose their type based on personal preference. It matters to you because it's your data that's being protected. You will want the best encryption type for the data you are storing or transmitting. This article tells about the practical application of such a data encryption method as AES in a tractor enterprise, which includes more than 50 personal computers with data that must be protected. Therefore, the article considers the method AES, a symmetric block cipher chosen by the U.S. government to protect classified information to be the best for company. AES is implemented in software and hardware throughout the world to encrypt sensitive data. It is essential for government computer security, cybersecurity and electronic data protection. Information security, sometimes shortened to InfoSec, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible.

Keywords: tractor factory, cyber security, encryption, algorithm, AES, access.

Introduction

Analysis of recent research and publications shows that Encryption methods vary by how much data they can handle at once and what kind of key it needs for its decryption. Some encryption is more easily hacked than others. While some companies or individuals choose encryption type according to standards dictated by legal or industrial regulations, others may simply choose their type based on personal preference. It matters to you because it's your data that's being protected. You will want the best encryption type for the data you are storing or transmitting.

The three major encryption types are DES, AES, and RSA. While there are many kinds of encryption - more than can easily be explained here - we will take a look at these three significant types of encryption that consumers use every day. Most of the others are variations on older types, and some are no longer supported or recommended. Tech is evolving every day and even those considered to be modern will be replaced by newer versions at some point.

Just as security tech is taking steps to increase the safety of your information, hackers are finding ways around them. It's an arms race with your data as the spoils of war. Let's dive in to popular encryption methods, the history of encryption, and where it's going next. [1]

The purpose of the article is to decide why the AES encryption method is the best for such a factory like tractor repair company

The main part of the article

Why should you use AES encryption? AES was developed to provide the highest level of security for the most sensitive data. The National Security Agency (NSA) and other agencies selected this method as the US government's security standard due to its extensive, impenetrable protection. AES is also used across many other government agencies and industries.

- Healthcare companies benefit from AES by encrypting their extensive databases of patient files, including medical history and personal information. The National Institute of Standards and Technology (NIST) recommends using AES to meet Health Insurance Portability and Accountability Act (HIPAA) regulations.
- Banks and other financial institutions rely on AES encryption to protect their customers' personal and transactional information.
- Insurance companies such as Aetna use AES to mitigate risk exposure in specific devices that are used to access customer information.

Even if your business doesn't fall under the umbrellas of government, healthcare, or finance, you can still employ the same level of security. Any precious information should be stored as safely as possible, and it might surprise you to know how many industries outside of the government have already adopted AES.

In fact, as of 2021, AES is the world's most popular data protection method.

Wi-Fi networks, Google Cloud, Facebook Messenger, Java programming, and many password managers use AES encryption to protect sensitive data.

This wide variety of applications shows that you can adapt AES for nearly any environment, and it's secure enough for even the most sensitive data [2].

Company description. Tolochyn Tractor repair company is a professional tractor repair association that offers repair services for:

- scheduled maintenance of the tractor;
- tractor engine overhaul;
- body restoration and repair;
- glow plug replacement
- tire and wheel replacement;
- front axle repair;
- hydraulic system;
- diagnostics;
- diagnostics and repair of the electronic part of the tractor;
- management and calculation of oil consumption;
- effective conversion of oil into electricity;

- development of oil production methods;
- management and efficient sale of oil.

The company includes the following departments: forge, welding, radiator department, mechanics department, electroplating department, tire shop, polymer department, secretary, general manager, unit repair, chief mechanic department. As you can see, the company has many departments that specialize in a certain area related to the repair of tractor units. each such department has personal computers that are connected via a network and have secret information that cannot be distributed outside the plant. Therefore, a method of data cryptography is needed for the enterprise

Equipment placement plan. On the Fig. 1 you can see equipment placement plan. As you can see, it is complicated due to company needs. According to the building plan, 78 computers, 2 printers, 6 MFPs and 1 server were placed.

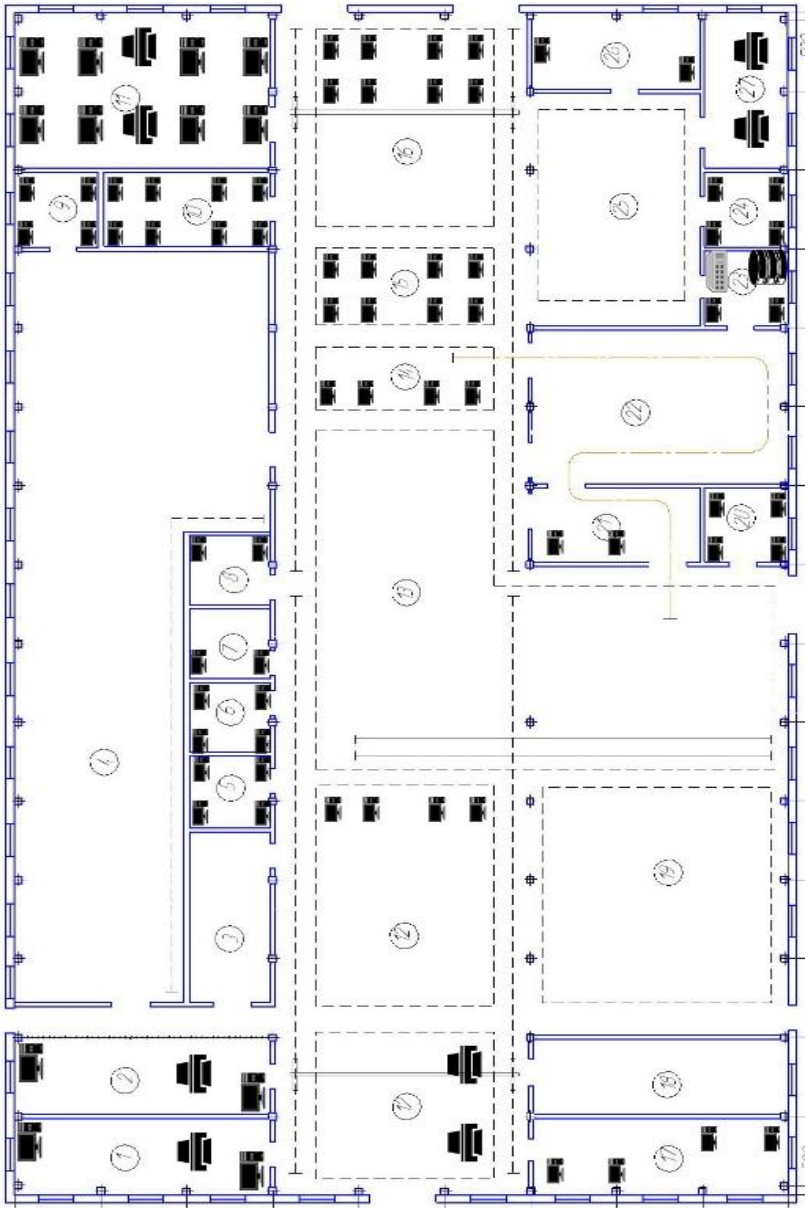

Fig. 1. Equipment placement plan

Data encryption at the enterprise. **Presentation of the application.** To encrypt data for the enterprise, it was chosen to develop a program that would encrypt and decrypt text using the AES (Advanced Encryption Standard, also known as Rijndael) cipher.

Advanced Encryption Standard is a symmetric block encryption algorithm (block size 128 bits, key 128/192/256 bits), a finalist in the AES competition and adopted as an American 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.

Advanced Encryption Standard (AES) is one of the most widely used and most secure encryption algorithms available today. It is publicly available and is the cipher used by the NSA to secure Top Secret documents. Its success story began in 1997, when NIST (National Institute of Standards and Technology) officially began looking for a replacement for the aging DES standard. The algorithm called Rijndael, developed by Belgian cryptographers

Daemen and Rijmen, was characterized by increased security, as well as performance and flexibility. [3]

It came out on top among several competitors and was officially announced in 2001 as the new AES encryption standard. The algorithm is based on multiple permutations, permutations, and linear transformations, each performed on 16-byte blocks of data, hence the term blockcipher. These operations are repeated several times, called "rounds". During each round, a unique round key is calculated from the encryption key and included in the calculations. Based on the block structure of AES, changing a single bit in either a key or a block of plaintext results in a different block of ciphertext - a clear advantage over traditional stream ciphers. Finally, the difference between AES-128, AES-192, and AES-256 is the key length: 128, 192, or 256 bits, all radical improvements over the 56-bit DES key. As an illustration, cracking a 128-bit AES key with a modern supercomputer would take longer than the estimated age of the universe. And Boxcryptor even uses 256-bit keys! To date, there is no real attack on AES. Therefore, AES remains the preferred encryption standard for governments, banks, and high-security systems around the world. Fig. 2 demonstrates how the method is working.

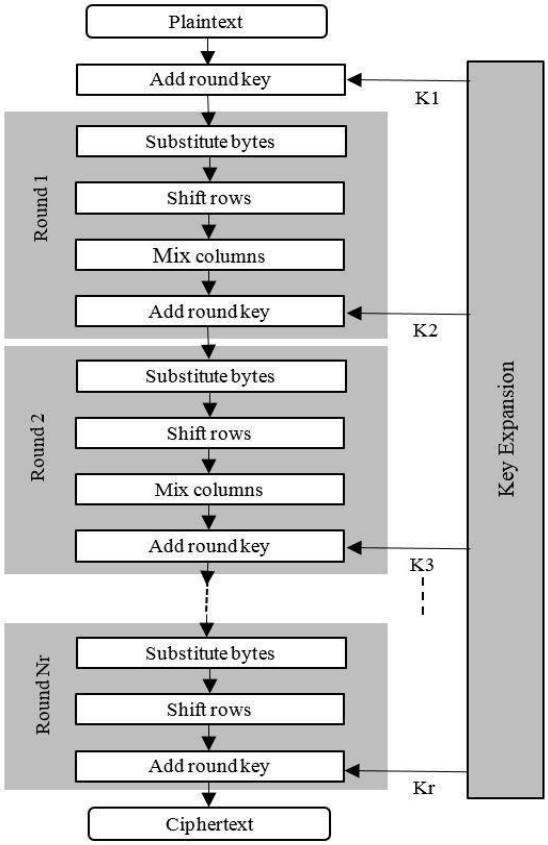

Fig. 2. Scheme of AES method

Brief overview of the created program for data encryption in the plant and its functions, initial window is on Fig. 3.

Text encryption is displayed on the Fig. 4. Text decoding by the program is shown on the Fig. 5.

The program also provides for cases when the user left the fields blank, for example encrypted text when decryption is required, or did not enter a numeric key. In such cases, the program will give a message explaining the error.

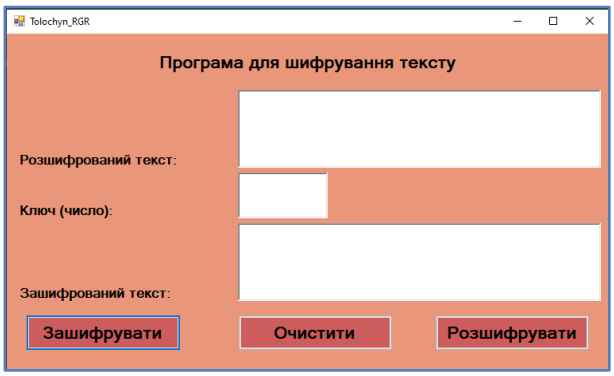

Fig. 3. Initial window of the program

Fig. 4. Text encryption process

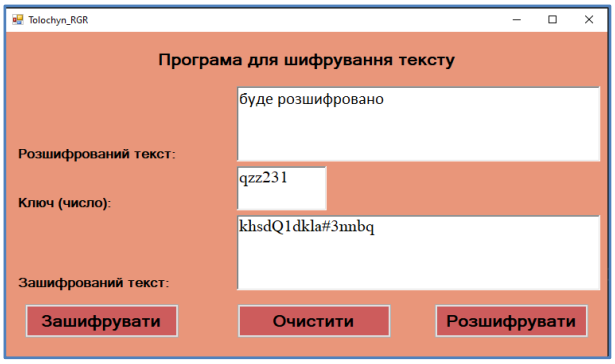

Fig. 5. Text decryption

The applications of the AES Encryption algorithm are as follows:

- Wireless Security: Wireless networks are secured using the Advanced Encryption Standard to authenticate routers and clients.
- WiFi networks have firmware software and complete security systems based on this algorithm and are now in everyday use.
- General File Encryption: Apart from corporate necessities, AES is also used to transfer files between associates in an encrypted format.

Conclusions

Information security, sometimes shortened to InfoSec, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information.

It also involves actions intended to reduce the adverse impacts of such incidents.

Protected information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity.

This is largely achieved through a structured risk management process [4].

Encrypting data in transit and data at rest helps ensure data confidentiality and integrity. Digital signatures are commonly used in cryptography to validate the authenticity of data. Cryptography and encryption has become increasingly important. A good example of cryptography use is the Advanced Encryption Standard (AES). The AES is a symmetric key algorithm used to protect classified government information [5].

In this particular case, a computer program was created to encrypt and decrypt important data of a tractor repair company that cannot be disclosed outside the company, based on such a data encryption method as AES.

REFERENCES

1. What Are the Different Types of Encryption?, URL: https://www.hp.com/us-en/shop/tech-takes/what-are-different-types-of-encryption#:~:text=The%20three%20major%20encryption%20types%20are%20DES%2C%20AES%2C%20and%20RSA
2. Is AES Encryption the Right Choice for Your Company?, URL: https://winzip.com/blog/enterprise/aes-encryption-explained
3. Data encryption using the XOR cypher G. Golovko, A. Matyashenko, N. Solopikhin - journal "Control, Navigation and Communication Systems". 2021. 81 p.
4. Information security, URL: https://en.wikipedia.org/wiki/Information_security
5. What Is Information Security, URL: https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html

Received (Надійшла) 05.09.2022
Accepted for publication (Прийнята до друку) 23.11.2022

Практичне застосування метода шифрування AES

Г. В. Головко, М. О. Толочин

Анотація. Аналіз останніх досліджень і публікацій показує, що методи шифрування відрізняються залежно від того, скільки даних вони можуть обробити одночасно та який ключ потрібен для їх дешифрування. Деякі засоби шифрування легше зламати, ніж інші. У той час як деякі компанії або окремі особи обирають тип шифрування відповідно до стандартів, що продиктовані юридичними чи промисловими нормами, інші можуть просто вибрати свій тип на основі особистих уподобань. Це важливо для вас, тому що ваші дані захищені. Вам потрібен найкращий тип шифрування для даних, які ви зберігаєте або передаєте. У цій статті розповідається про практичне застосування такого методу шифрування даних, як AES, на тракторному підприємстві, яке включає понад 50 персональних комп'ютерів з даними, які необхідно захищати. Тому в статті найкращим для компанії вважається метод AES, симетричний блоковий шифр, обраний урядом США для захисту секретної інформації. AES реалізовано в програмному та апаратному забезпеченні по всьому світу для шифрування конфіденційних даних. Це має важливе значення для комп'ютерної безпеки уряду, кібербезпеки та захисту електронних даних. Інформаційна безпека, іноді скорочена до InfoSec, — це практика захисту інформації шляхом зменшення інформаційних ризиків. Це частина управління інформаційними ризиками. Зазвичай це передбачає запобігання або зменшення ймовірності несанкціонованого/неналежного доступу до даних або незаконного використання, розголошення, порушення, видалення, пошкодження, модифікації, перевірки, запису або знецінення інформації. Це також передбачає дії, спрямовані на зменшення негативних наслідків таких інцидентів. Захищена інформація може мати будь-яку форму, напр. електронні або фізичні, матеріальні (наприклад, документи) або нематеріальні.

Ключові слова: тракторний завод, кібербезпека, шифрування, алгоритм, AES, доступ.