UDC 004.9 **doi: 10.26906/SUNZ.2021.1.081**

G. Golovko, A. Matiashenko, N. Solopihin

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

DATA ENCRYPTION USING XOR CIPHER

Abstract. This article offers an example of using an application whose main task is to encrypt data such as files and private messages. Data encryption is performed using an encryption algorithm - xor. The XOR cipher is a data encryption algorithm using exclusive disjunction. Acquired widespread use in computer networks in the 90's due to the ease of implementation. Used to encrypt Microsoft Word documents in Windows. The XOR encryption algorithm is to "overlay" a sequence of random numbers on the text to be encrypted. A sequence of random numbers is called a gamma sequence, and is used to encrypt and decrypt data. If you use a key with a length at least equal to the length of the message, the XOR cipher becomes much more crypto-resistant than when using a duplicate key. For cryptological protection of information of the travel company Rest & Travel, EDcrypt software has been created, which performs the following functions: account login; inability to use the system without logging in to the account; notification of entering incorrect user data; message encryption; decryption of messages; the ability to select the recipient of the message; encryption of text files; decryption of text files; sending text files to selected recipients; three interface languages: English, Russian, Ukrainian.

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

Introduction

People tend to protect their secrets. The development of information technologies, their penetration into all spheres of human activity leads to the fact that the problems of information security are becoming more and more relevant every year - and at the same time more complex. There are no universal methods of protection, in many respects the success in building security mechanisms for a real system will depend on its individual characteristics, the account of which is difficult to formalize. Therefore, information security is often considered as a set of informal recommendations for building information security systems of one type or another. However, the practical methods of building protection systems are general laws that do not depend on the technical features of their implementation.

Information security is a multifaceted area of activity in which only a systematic, comprehensive approach can bring success. The range of interests of the subjects connected with use of information systems can be divided into the following categories:

• ensuring accessibility;

• integrity;

• confidentiality of information resources and infrastructure that supports it [1].

Information security is the protection of information from negative influences on it and it is related to technological procedures to ensure protection.

Confidentiality of information is the status of information, which is fixed depending on its importance and requires a certain level of protection. Thus, this concept refers to people, individuals who are responsible for information and decide what information can be disclosed and what to hide from other people.

In fact, the field of information security is not the protection of information, but the protection of property rights to it.

Information is not a material object, information is knowledge, a reflection of reality in the human mind. And only in the future information can be embodied in the material objects of the world around us. However, not being a material object, information is inextricably linked to the material carrier: it is the human brain or alienated from human material carriers.

Why the problem of using cryptographic methods in information systems has become especially relevant at the moment:

• on the one hand, the use of computer networks has expanded, in particular the global Internet, which transmits large amounts of information of state, military, commercial nature, which prevents the possibility of access to it by outsiders;

• on the other hand, the emergence of new powerful computers, network and neural computing technologies.

Cryptology (kryptos - secret, logos - science) deals with the problem of information protection by its transformation. Cryptology is divided into two areas - cryptography and cryptanalysis. The goals of these areas are exactly the opposite.

Cryptographic information security system is a set of cryptographic algorithms, protocols and procedures for the formation, distribution, transmission and use of cryptographic keys [2].

Code - a set of algorithms for cryptographic transformations (encryption), reflecting the set of possible open data on the set of possible encrypted data, and their inverse transformations. An important parameter of any cipher is a key - a parameter of a cryptographic algorithm that provides a choice of one transformation from the set of transformations possible for this algorithm. In modern cryptography, it is assumed that all the secrecy of the cryptographic algorithm is concentrated in the key, but not in the details of the algorithm (Kirkhoffs principle) [1].

If all of the cryptographic functions stopped working for a day, modern life as we know it would stop. Bank transactions wouldn't go through, internet traffic would come to a halt, and cell phones would no longer function. At this point, all of our important information would be exposed, and it then could be exploited to do unimaginable harm to us all.

Cryptography makes it possible to convert information in such a way that its reading (recovery) is

possible only with the knowledge of the key. Texts based on some alphabet will be considered as information to be encrypted and decrypted [2].

Cryptography is an essential way of preventing that from happening. It secures information and communications using a set of rules that allows only those intended and no one else to receive the information to access and process it.

Analysis of recent research and publications. In our day-to-day lives, the use of cryptography is everywhere. For example, we use it to securely send passwords over vast networks for online purchases. Bank servers and e-mail clients save your passwords using cryptography as well. Cryptography is used to secure all transmitted information in our IoT-connected world, to authenticate people and devices, and devices to other devices.

In computer science, cryptography refers to secure information and communication techniques derived from mathematical concepts and a set of rule-based calculations called algorithms, to transform messages in ways that are hard to decipher. These deterministic algorithms are used for cryptographic key generation, digital signing, verification to protect data privacy, web browsing on the internet, and confidential communications such as credit card transactions and email [6].

The main part of the article

Cryptography is closely related to the disciplines of cryptology and cryptanalysis. It includes techniques such as microdots, merging words with images, and other ways to hide information in storage or transit. However, in today's computer-centric world, cryptography is most often associated with scrambling plaintext (ordinary text, sometimes referred to as cleartext) into ciphertext (a process called encryption), then back again (known as decryption). Individuals who practice this field are known as cryptographers.

Modern cryptography concerns itself with the following four objectives:

1. Confidentiality: the information cannot be understood by anyone for whom it was unintended.

2. Integrity: the information cannot be altered in storage or transit between sender and intended receiver without the alteration being detected.

3. Non-repudiation: the creator/sender of the information cannot deny at a later stage his or her intentions in the creation or transmission of the information.

4. Authentication: the sender and receiver can confirm each other's identity and the origin/destination of the information [1].

The XOR cipher. Simply put, XOR (pronounced “exclusive or”) cipher is an additive cypher. It is based on the XOR operation (also known as the exclusive disjunction) in logic.

As a logical operation, XOR is also called modulus 2 additions. In XOR operation, the output is true when the inputs differ. In other words, XOR operation means “either one but not both or none” [3].

The XOR cipher is often used in computer malware to make reverse engineering more difficult.

If the key is random and is at least as long as the message, the XOR cipher is much more secure than when there is key repetition within a message [2].

The XOR Encryption algorithm is a very effective yet easy to implement method of symmetric encryption. Due to its effectiveness and simplicity, the XOR Encryption is an extremely common component used in more complex encryption algorithms used nowadays.

The XOR encryption algorithm is an example of symmetric encryption where the same key is used to both encrypt and decrypt a message.

The XOR Encryption algorithm is based on applying an XOR mask using the plaintext and a key [4].

Using the example of an application created to encrypt messages and files that are exchanged by Rest&Travel employees, you can see how XOR encryption actually works [7].

After starting the program, we see the login window, if you do not enter the password and login, the program will not allow you to continue working. (Fig. 1). Enter the system (Fig. 2). If the login and/or password is entered incorrectly, the program notifies us and deletes the entered user data.

Fig. 1. Choice of interface system

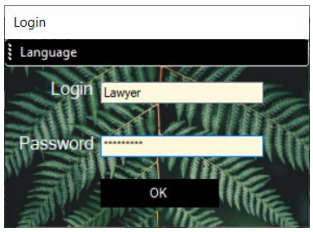

Fig. 2. Login to the language

After log in in the main menu we see our login, the account from which we will perform certain actions. We can choose what we want to send messages or files (Fig. 3).

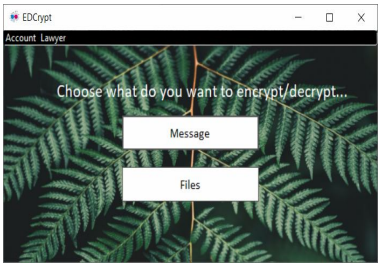

Fig. 3. Main window

To send a message, all we have to do is choose who we want to send the message to, enter the password to encrypt the data, enter the message text and the subject of the message. Similarly, to decrypt data, we only need to enter the encrypted text and send it to the desired user, such as yourself (Fig. 4–6).

To encrypt text files, we need to enter the encryption password, choose where to save the file, enter the subject or file name and click the desired button, then download the file, it is encrypted or decrypted automatically and saved depending on the selected direction (Fig. 7, 8).

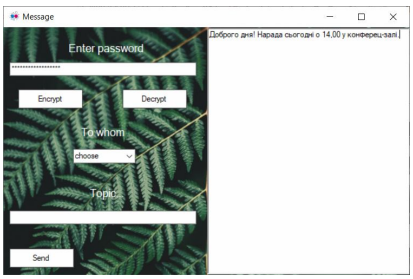

Fig. 4. Sending a message

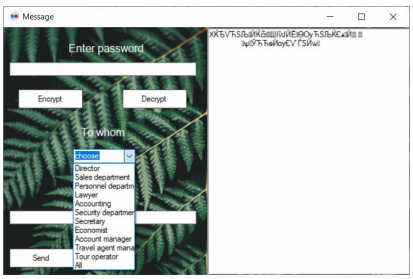

Fig. 5. Recipient selection

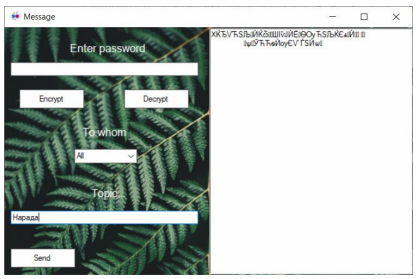

Fig. 6. Sending an encrypted message

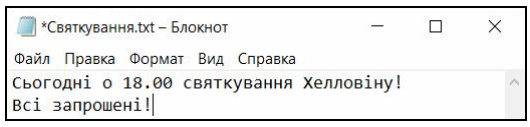

Fig. 7. The contents of the file before encryption

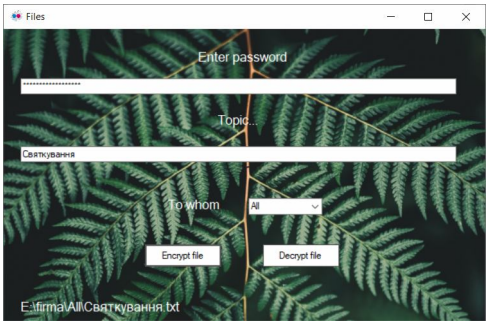

Fig. 8. Upload and encrypt file

Conclusions

Information security - measures taken to prevent unauthorized use, misuse, alteration of information, facts, data or hardware or denial of access to them. As can be seen from the definition, information security does not provide absolute protection. As a result of the study it was determined when XOR cipher has a random key that is as long as the message itself, it is impossible to crack it. In other words, it offers the highest level of security. When a large quantity of text is to be encrypted, a shorter repeating encryption key is used to match the length of the plain text. However re-using the same key over and over, or using a shorter repeating key results in a less secure method where the cipher text could be decrypted using a frequency analysis.

A significant part of the problems of information security can be solved by organizational measures. However, with the development of information technology there is a tendency to increase the use of technical protection measures and software, including cryptological. At present, crypto-logical protection of information is the most perfect type of restriction of access to data and therefore its use is relevant and necessary. Information security is a precautionary measure that protects information and equipment from threats and the use of their vulnerabilities.

Was created the program to encrypt messages and files that are exchanged by Rest&Travel employees.

REFERENCES

1. Search security, Cryptography, URL: https://searchsecurity.techtarget.com/definition/
2. Churchhouse, Robert (2002), Codes and Ciphers: Julius Caesar, the Enigma and the Internet, Cambridge: CU Press.
3. Logsign, How Does XOR Cipher Work?. URL: https://www.logsign.com/blog/how-does-xor-cipher-work/
4. 101 copmuting, XOR Encryption Algorithm, URL: https://www.101computing.net/xor-encryption-algorithm/
5. Programming algorithms, XOR Encryption, URL: https://www.programmingalgorithms.com/algorithm/xor-encryption/
6. Electronic design, Cryptography: Why Do We Need It? , URL: https://www.electronicdesign.com/technologies/embedded-revolution/article/21127827.
7. Golovko G. V., Nikiforova K. M. Information systems use at Poltava national technical Yuri Kondratyuk University. *Control, navigation and communication systems*. 2018. Vol. 3. P. 103-105.

Received (Надійшла) 12.11.2020
Accepted for publication (Прийнята до друку) 03.02.2021

Шифрування даних за допомогою алгоритму шифрування XOR

Г. Головко, А. Матяшенко, Н. Солопіхін

Анотація. Запропоновано приклад використання додатку, головною задачею якої є шифрування даних, таких як - файли та приватні повідомлення. Шифрування даних відбувається за допомогою алгоритму шифрування - xor. Шифр XOR – це алгоритм шифрування даних з використанням виключної диз'юнкції. Набув широкого застосування у комп'ютерних мережах 90-х років у зв'язку зі простотою реалізації. Застосовувався для шифрування документів Microsoft Word в середовищі Windows. Алгоритм XOR шифрування полягає в "накладанні" послідовності випадкових чисел на текст, який необхідно зашифрувати. Послідовність випадкових чисел називається гама-послідовність, та використовується для шифрування та розшифрування даних. Якщо використовується ключ довжиною, як найменше, рівний довжині повідомлення, то шифр XOR стає значно більш криптостійким, ніж при використанні ключа, що повторюється. Для криптологічного захисту інформації туристичної компанії Rest&Travel створено програмне забезпечення EDcrypt, що виконує такі функції: вхід за обліковим записом; неможливість користування системою без входу за обліковим записом; повідомлення про введення некоректних даних про користувача; шифрування повідомлень; розшифрування повідомлень; можливість вибору отримувача повідомлення; шифрування текстових файлів; розшифрування текстових файлів; розсилання текстових файлів вибраним отримувачам; три мови інтерфейсу: англійська, російська, українська.

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