POPOVYCH YAROSLAV

DEVELOPMENT OF AN ENCRYPTION SYSTEM IN CLOUD DATA STORAGE

UNESCO — UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION

JUNIOR ACADEMY OF SCIENCES OF UKRAINE UNDER THE AUSPICES OF UNESCO

Introduction

Cloud storage is now widely used. Many people use cloud storage to store their data, so they need good protection. It was created to protect information and there was developed an encryption system that has been tested on the example of console chat and website which encrypts data on Google Drive in real time.

The purpose of the study is to increase the efficiency of encryption of large messages in cloud data storage.

The problems of the study are analysis of existing encryption algorithms; development of a new algorithm that combines the advantages of block and table ciphers; analysis of the work of existing and developed ciphers in time and crypto currency; testing of a new algorithm; development of encryption system; creating a chat; creating a website; using system of encryption in console chat and website for encoding data on Google Drive.

Research methods: studying the experience of specialists, analysis and comparison.

The object of study is the process of rapid encryption of large amount of data.

Subjects of research are mathematical models and methods of fast encryption of large messages.

Conclusion

Results: existing encryption algorithms had been studied and analyzed; written own algorithm and data encryption system; the comparative analysis of the developed algorithm with already known is carried out; the crypto analysis of the developed algorithm is carried out; developed a prototype of a chat and a program for encryption and data transfer to cloud storage in real time; testing of the developed encryption system on the example of written chat and site-program

To sum up, for storing large files in cloud data storage, the developed cipher proved to be the best, due to the ability to control the running time of the algorithm and its cryptographic stability. This algorithm has more reliable crypto currency compared to the Vigenere cipher, does not require the generation of a large number of random numbers, like the Vernam cipher, and works much faster than the DES cipher.

In practice, this work can be used to securely send large messages for save in cloud storage using technique of any capacity.

In future, instead of the Vigenere cipher, I can take other ciphers that work in linear time, optimize the developed cipher for them and find better solution.

Algorithms

The developed algorithm divides open text into a couple of blocks with the length of the key. Then, on the first round it encodes first block using the Vigenere cipher with the initialization vector which equals value of the key. Each of the following blocks encodes using initialization vector as previous encoded block. On every next round first block uses the last cipher block as initialization vector. The working scheme is illustrated in Figure 1.

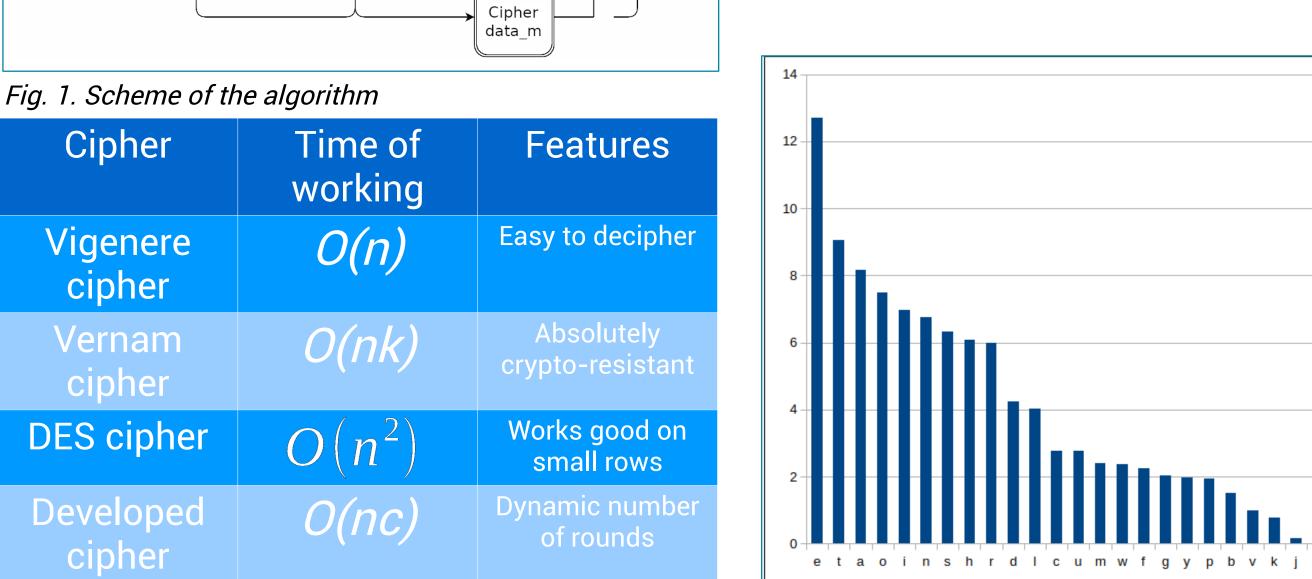*Fig. 2. Approximate time of working of algorithms (blue − Vigenere, green − mine, purple − Vernam, red - DES)*

The Vigenere algorithm work in linear time, which is fast enough, but there is a way to decode it, so it is useless to use it without other constructions. The Vernam algorithm is the only absolutely crypto-resistant cipher as we can see in Table 1, but it can not be used in chat, because it needs generation and sharing of big amount of random numbers. The DES algorithm is extremely good on small rows, but on long rows it works too long.

Time of working of developed algorithm can be changed as well as its crypto-resistance, because of dynamic amount of rounds, which is shown on Figure 2.

There were made a couple of tests of crypto-resistance of developed algorithm. It shows results much better than Vigenere cipher and it is enough to share big amounts of data. For example there is a method which uses probability of appearance of each symbol in text. Figure 3 shows an example of such probabilities.

Fig. 1. Scheme of the algorithm

Cipher	Time of working	Features
Vigenere cipher	$O(n)$	Easy to decipher
Vernam cipher	$O(nk)$	Absolutely crypto-resistant
DES cipher	$O(n^2)$	Works good on small rows
Developed cipher	$O(nc)$	Dynamic number of rounds

Table 1. Algorithm comparing

Fig. 3. Probability of appearance of each symbol

Programs

Fig. 4. How developed algorithm works during encrypting and decoding data on 3 rounds

This algorithm encodes or decodes data depending on entered number (0 or 1). After that, program asks person to enter path of file with inputted text, and path where to write the result, as you can see in Figure 4.

Figure 5 represents how developed console chat works. Firstly, person who wants to send a message encrypts data on his side, than data comes to server, writes into database, and each other participant of his group asks server to send a message to decrypt it. Such scheme provides security for users and cancels possibility of stealing data from server side.

Fig. 5. Scheme of chat work

Figure 6 illustrates three clients who are creating two groups and connecting to them. The chat shows an ability to share messages, also it shows when participant connects and disconnects from the group. Also Table between upper and bottom figures presents an example which could be seen on server side during sending message "*Hello, my name is Sam. login − admin, password − admin*" using key which equals "*secret pass*" on 100 rounds.
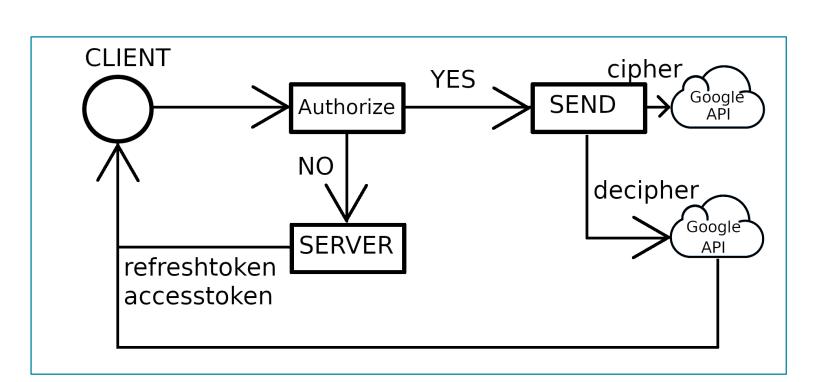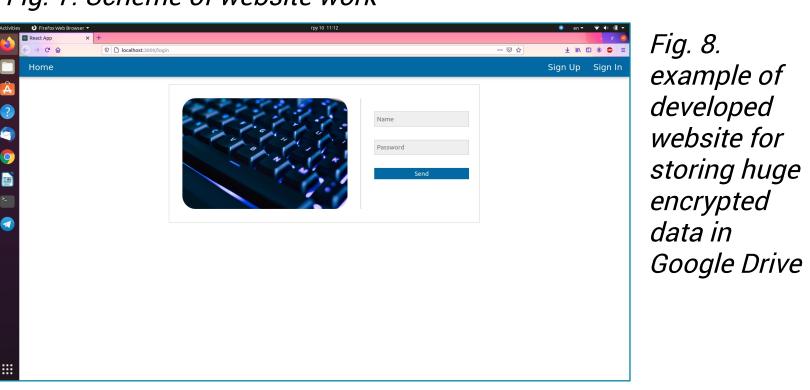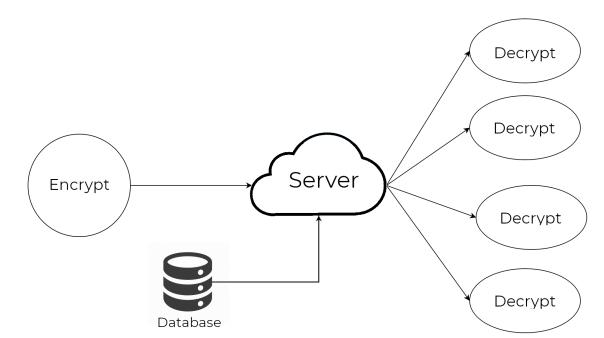
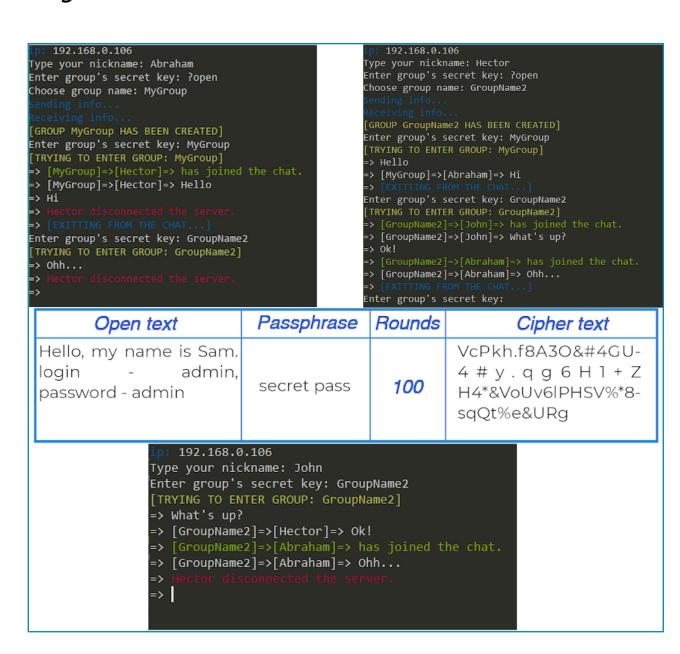| Open text	Passphrase	Rounds	Cipher text
Hello, my name is Sam. login − admin, password - admin	secret pass	100	VcPkh.f8A3O&#4GU-4 # y . q g 6 H 1 + Z H4*&VoUv6lPHSV%*8-sqQt%e&URg

Fig. 6. example of chat work and encryption data on 100 rounds

In Figure 7 it is illustrated scheme of website working. First of all, user have to authorize. Unless user is authorized he will not be able to see the content of website. Further, client can exchange encrypted data with Google Drive, so that the data will not be understandable for Google.

Fig. 7. Scheme of website work

Fig. 8. example of developed website for storing huge encrypted data in Google Drive

Figure 8 shows a prototype of developed website for storing big amounts of data to Google Drive. The website uses JWT (Json Web Token) for authentication, so that the website could be expanded into different servers to parallelize tasks and to optimize whole system.