Development of an import–substituting software package for secure file transfer, based on the modified protocol of EL–GAMAL

Larisa Cherckesova[1], *Olga* Safaryan[1*], *Nikolay* Boldyrikhin[1], *Boris* Akishin[1], and *Vasiliy* Yukhnov[2]

[1] Don State Technical University, Gagarin Square, 1, Rostov-on-Don, 344003, Russia
[2] Rostov State Transport University, square of the Rostov Rifle Regiment of the People's Militia, 2, Rostov-on-Don, 344038, Russia

Abstract. The article describes the development of modified encryption protocol based on the El–Gamal cryptoalgorithm. The development of an import–substituting software package for secure file transfer, based on the modified protocol of El–Gamal was made also.

1 Introduction

In today's world of globalization and development of information technology, it is not possible to build a business and production without using the latest advances in science and technology related to information technology. Moreover, today the development of an appropriate regulatory framework in the Russian Federation strengthens the process of introducing this type of technology into the modern market. The most promising branches of the direction of information technology are the development and application of cryptographic means of protecting information for various purposes, including the use by government bodies and commercial organizations, the implementation of electronic document management tools, the expansion of the use of encryption schemes based on public keys and means of protecting web resources from various attacks [1].

Among the advantages of using this kind of technology are: more efficient office management, which is achieved by reducing the likelihood of distortion of transmitted information, as well as its damage and loss, less time for transmission of information packets over the network, as well as optimization of search capabilities of the corresponding aggregators, which makes it possible to the user in the shortest possible time to receive the required data. Moreover, the introduction into operation of an electronic digital signature as a cryptographic system is capable of fully ensuring the implementation of the basic properties of information: integrity and confidentiality. However, at the same time, this use does not provide guarantees for the provision of another important property of information resources – accessibility.

* Corresponding author: safari_2006@mail.ru

In this case, in order to have the possibility of continuous access to conditional certification centers from the users of the system, it is necessary to ensure the trouble-free operation of the infrastructure service that processes and generates public keys.

Thus, the problem of countering and repelling attacks on the ongoing data exchange is an urgent problem due to the complexity of ensuring a 100% level of protection of corporate information systems, while correctly prioritizing data protection tasks in the context of a limited budget share directed to information technology.

Encryption algorithms are designed to solve the problem of ensuring the confidentiality of information. [2-4]. Currently, cryptographic methods are used extensively to close information. Since ancient times, encryption has been and remains the most effective form of protection. Encryption is defined as the inverse transformation of unprotected (open) information into an encrypted (closed) form – ciphertext, in which it is not fully accessible to the attacker. During encryption, keys are used, the presence of which means the ability to encrypt and/or decrypt information. It is important to note that the encryption method itself is not required to be kept secret, since knowing only it will not allow decrypting the ciphertext [5-7].

The purpose of this article is the practical implementation of software tool for secret data transmission based on the modified El–Gamal protocol.

The asymmetric El–Gamal scheme uses the exponentiation operation modulo of prime number. In this case, the difficult task for an attacker is not to find a number that was raised to a power, but to what degree is the number raised. This problem is called the discrete logarithm problem [2].

2 Description of the work of the import-substituting software package for secure file transfer

In the modern society of information communications, it is especially important to pay attention to the implementation of file sharing, namely: it is important to control the data that users are trying to transmit. Among the variety of such files, the virus files with malicious software may be involved. Therefore, an attacker under the guise of an ordinary user can intercept protected information by sending the virus to the client.

To prevent this, it was decided to develop an algorithm that would check the files for the presence of malicious software in the files before uploading them to the server in encrypted form. This action must be performed just before encrypting the file, because if the information is encrypted, then no antivirus will be able to detect the presence of the threat in the file, since the information in this file is already distorted.

To develop a software tool, requirements were formulated for the characteristics of the program itself. These include a fast, reliable and secure platform for secret encrypted file sharing and operating system compatibility. It is also important to provide restricted access to certain encrypted files.

The HTTP protocol is used to transfer data. It is needed to communicate with a remote server and then send files from the local computer to the remote server, and ultimately to the server of the recipient of the transferred files.

The general principle of the program is based on the fact that the exchange of files between clients occurs through a server that is publicly available on the Internet. On this server, the numbers p and g-parameters of our system are initially fixed. Next, the user launches the program on the local computer; the application automatically sends a request to the server and receives the system parameters.

Then, on the client's computer, a random integer coprime with (p-1) number x is selected that satisfies the condition 1 <x <p-1. Thus, the private key of client x is generated. The next step is to calculate the public key y using the formula:

$$y=q^x \bmod p. \quad (1)$$

Modification of the cryptographic algorithm of El–Gamal is described by the ratio:

$$p=b*q+1 \quad (2)$$

The highest bits of p and q must be equal to one, then such number is selected a>1, such, that:

$$a^q \bmod p = 1. \quad (3)$$

The result is three–p option q and a [3, 4].

Since the secrecy of data transmission is important to user, and the attackers can intercept and read the transmitted files, we must protect ourselves from such risks. To ensure the comprehensive protection when using the program, you must use the encryption method of the transmitted files.

At the first stage of the program, a new user is created by entering information about the client and a login is assigned. This information is entered into a file on the client's local computer, and the entered information is also added to the general database. This data is stored on a secure server, which delimits access rights by client authentication. Then the function of selecting files for their subsequent sending is called. The function, in turn, calls the file encryption subfunction. At this stage of the program, the selected file is encrypted before sending it using the modified El - Gamal scheme. After the file is encrypted, via the HTTP protocol, it is transferred to the server for storage in an inaccessible form for any intruders.

Even if an attacker intercepts the transmitted data, he will not be able to extract any information from these files. data encrypted by the modified El–Gamal method [5, 7–9].

Now there is a transfer from the client device to the server of the public key y and his login at the same time. The server sends the received data to the database, which records information about all clients that are registered in this program. The key exchange the block diagram is shown in Fig. 3.

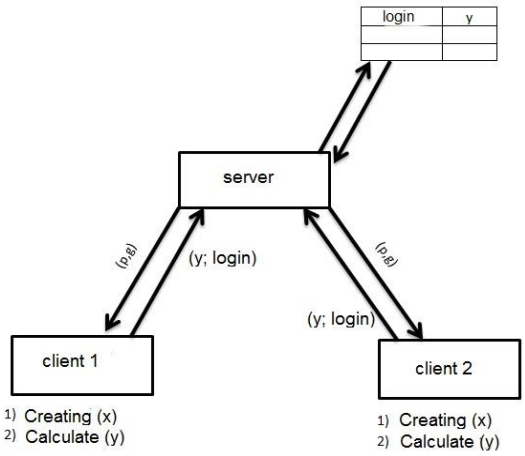

Fig. 1. Key exchange mechanism functioning diagram.

The modified El-Gamal method provides secure data exchange due to the following two elements: authentication, encryption. This method involves creating a private key that is known to only one user and does not need to be passed on to anyone. And the authentication channel will only allow certain individuals to gain access to files. The welcome window contains information about the user (Fig. 2).

Fig. 2. Welcome window.

In order to protect all users who will use the developed product, all sent files are scanned for the presence of malicious software. To do this, before encrypting the file and uploading it to the server, the VirusTotal service is contacted by sending the hash of the client's file to a public service. If a confirmation comes that the file contains malware, the client will be denied to send the file [10-13].

VirusTotal is the free service that analyzes suspicious files and links (URLs) for viruses, worms, Trojans, and all kinds of malware. The results of file checks by the service do not depend on any one antivirus manufacturer. VirusTotal uses several dozen antivirus systems, which will allow you to make more reliable conclusions about the danger of a file (if all or most antiviruses consider the file dangerous), compared to a single product, it can help to assume possible false positives of a single antivirus (or antiviruses), or, conversely, failure to respond to a fresh threat, possibly already entered by other manufacturers in their databases.

In the developed software tool for secure file transfer, it was implemented to check the sent files for malicious software by calculating the checksum of the file prepared for sending and sending a request with the calculated amount to the VirusTotal server. If the response from the server contains information that the file contains a virus, the program immediately displays a message to the user who wanted to transfer the file, stating that the transferred file contains a virus and its transfer is impossible.

In order for a user to send a file to another user, it first sends a request with the client's login to the server to get the public key y of the client that needs to receive the file in response. The sender, knowing the public key of the recipient, encrypts the transmitted files using the received y from the server according to the El-Gamal scheme and subsequently uploads the already encrypted file to the server. All information about the files and who they belong to is entered in the database. At the same time, the recipient receives a notification on the computer that the server has received a file for the specified username and offers to download it. The selection of files to upload files to is shown in Fig. 3.

The search for clients is shown in Fig. 4.

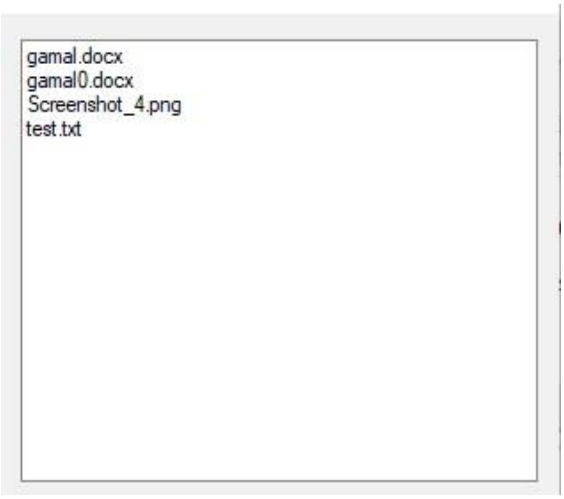

Fig. 3. Display files for download.

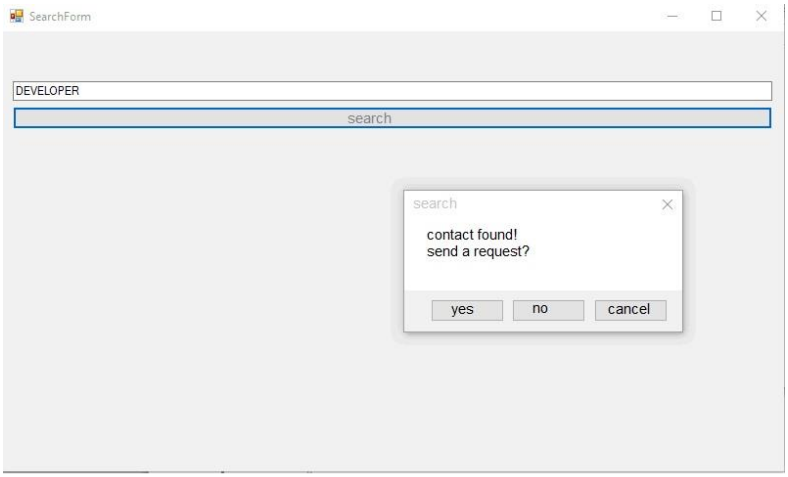

Fig. 4. Client search.

After receiving the file by the addressee using his private key, the received file is decrypted for further use for his own purposes. If an attacker gains access to a file by intercepting the file on the server, then he will not be able to gain access to the information contained in it, since the attacker does not know the secret key x of the client to which the file was addressed. The private key is unknown to anyone other than the client. For additional security, access to files will be carried out only by the recipient to whom this file is intended. The file transfer scheme is shown in Fig. 5.

After launching the software package, the main program window will appear on the screen, which contains the client registration menu and subsequent operations for receiving and sending files, as well as for checking files before sending [13 – 15].

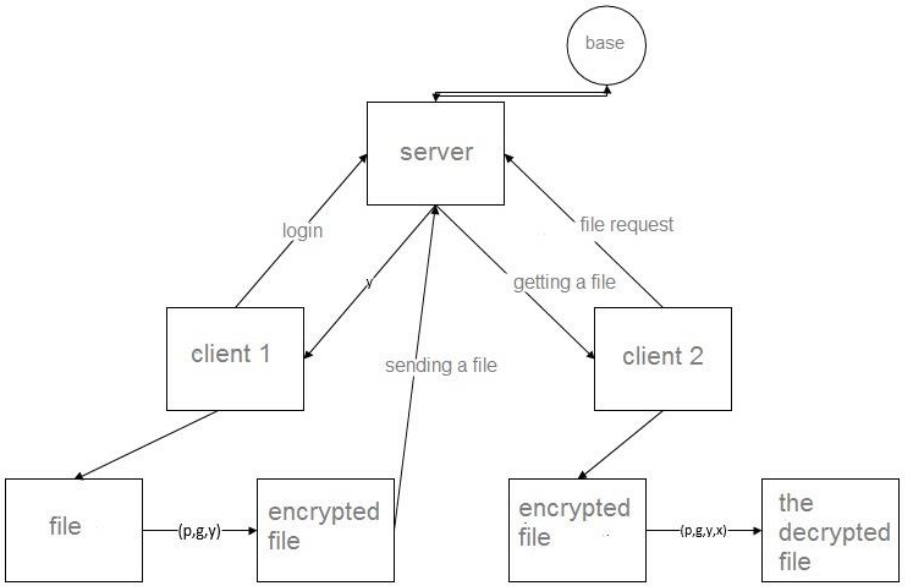

Fig. 5. File transfer.

The program transfers files to the server in encrypted form, addressed only to a specific contact. The second user gains access to the file, downloads it to his computer, and then the file is decrypted to gain access to the information in it. The private key is not transferred, this gives an advantage in the security of file exchange compared to analogs.

3 Discussion and conclusions

In this work, a software tool was developed that implements a modified El-Gamal encryption algorithm. The advantage of this software is the ability to authenticate the subject, protection against replay, hidden recipient authentication, confidentiality, ensuring anonymity at work, checking files before sending, a friendly software interface that is available when launched from any device, increased encryption speed, stability of operation, increased cryptographic strength algorithm in comparison with analogues.

References

1. V.S.Tabar, S. Ghassemzadeh, S. Tohidi, Energy, **220**, 119776 (2021), https://doi.org/10.1016/ j.energy. 2021. 119776
2. B.G. Ibrahimov, R.T. Humbatov, R. F. Ibrahimov, IFAC–PapersOnLine, **51(30)**, 821 – 824 (2018), https://doi.org/10.1016/j.ifacol. 2018. 11.187
3. V.V. Zhilin, I.I. Drozdova, I.A. Sakharov, et al., in Proceedings of IEEE East–West Design and Test Symposium, EWDTS 2019, Institute of Electrical and Electronics Engineers Inc., 8884375 (2019), DOI: 10.1109/EWDTS.2019.8884375
4. A.A. Afanasyev, Authentication. Theory and practice of providing secure access to information resources. Textbook for universities (Hot Line – Telecom, Moscow, 2012)
5. E. Rostami, F. Karlsson, S. Gao, Computers & Security, **99**, 102063 (2020),

https://doi.org/10.1016/j.cose.2020.102063

6. A. P.Bhatt, A. Sharma, Journal of Electronic Science and Technology, **17(3)**, 213 – 220 (2019), https://doi.org/10.11989/JEST.1674-862X.90523016
7. J. Kaur, K.R. Ramkumar, Journal of King Saud University - Computer and Information Sciences (2021), https://doi.org/10.1016/j.jksuci.2021.01.018
8. O.A. Imran, S.F. Yousif, I.S. Hameed, et al., Procedia Computer Science, **167**, 1028–1037 (2020)
9. F.M. Salem, R. Amin, Information Sciences, **527**, 382 – 393 (2020)
10. K. Kularbphettong, R. Putglan, N. Tachpetpaiboon, et al., Procedia – Social and Behavioral Sciences, **197**, 793 – 796 (2015), https://doi.org/10.1016/j.sbspro.2015.07.184
11. O.A. Imran, S. F. Yousif, I.S. Hameed, et al., Procedia Computer Science, 167, 1028–1037 (2020), https://doi.org/10.1016/j.procs.2020.03.402
12. N. Okumura, K. Ogata, Y. Shinoda, Journal of Information Security and Applications, **53**, 102529 (2020)
13. A.A. Mauro, Joel J.P.C.Rodrigues, P. Lorenz, et al., Future Generation Computer Systems, **97**, 145–152 (2019)
14. N. Okumura, K. Ogata, Y. Shinoda, Journal of Information Security and Applications, **53**, 102529 (2020), https://doi.org/ 10.1016/ j.jisa.2020.102529
15. E.S. Alashwaliab, P. Szalachowskic, A. Martinan, Computers & Security, 97, 101975 (2020), https://doi.org/ 10.1016/ j.cose.2020.101975