UDC 004.223.2

PROTECTED TRANSFER OF MESSAGES BETWEEN USERS ON THE BASIS OF POST-QUANTUM CRYPTOGRAPHY

V. PETYUKEVICH, D. PASTUKHOV
Polotsk State University, Belarus

The article discusses the design of a secure data transfer scheme between users according to the peer-to-peer scheme, as well as the issues of protecting this data. The analysis of the technologies most suitable for the development of this scheme.

Some means of transferring information between users, such as Viber and Telegram, use message encryption, but transmit messages through their own servers. Thus, it turns out that all user messages can be stored on the server and, subsequently, be transmitted to someone.

There are two primary problems: the problem of intercepting transmitted data, the vulnerability of encryption algorithms to cryptographic attacks. These problems can be solved using public key cryptosystems and peer-to-peer connections.

A peer-to-peer network is an overlaying computer network based on equal rights of participants. Often there are no dedicated servers in such a network, and each node (peer) is both a client and acts as a server. Unlike the client-server architecture, such an organization allows the network to remain operable with any number and any combination of available nodes. Members of the network are peers. [1]

Benefits from using peer-to-peer:

1. Protection against server data leakage;
2. Reducing the load on the application server, because the server will cease to participate in the process of sending messages.

Existing solutions. None of the popular messaging tools use message protection at the highest possible level. Viber and Telegram use end-to-end encryption, but their common problem is control of the entire message passing process by the servers of these services.

Ent-to-end encryption is a data transfer method in which only users participating in communication have access to messages. Thus, the use of pass-through encryption does not allow access to the cryptographic keys by third parties. [2]

The topic of combining end-to-end encryption and peer-to-peer connections is not well developed. Only one article in English was found on the Internet. But in this article only theoretical issues were considered without considering the options of the technologies used.

Means of solving the problem. This article deals only with the case of the transfer of text data. However, the technologies used in this scheme can be applied to transfer other types of data.

A public key cryptographic system allows encrypting messages with a public key that can be transmitted over insecure channels. The NTRUEncrypt algorithm was chosen as a public-key cryptographic system.

In addition to solving the problem of intercepting transmitted data, NTRUEncrypt solves the urgent problem of instability of traditional encryption algorithms, such as RSA, to the Shore algorithm. The Shore algorithm allows solving the factorization problems of integers or the discrete logarithm problem using a quantum computer. In turn, NTRUEncrypt is based on a trellised cryptosystem. The stability of the algorithm is provided by the difficulty of finding the shortest lattice vector. Unlike its predecessors, the NTRU does not work on a residue ring modulo an integer N , but on a ring of polynomials of degree $n-1$, reduced modulo x^n-1 . Addition of elements in such a group occurs as usual addition, and when multiplying, the element x^n is reduced to 1, x^{n+1} to x , and so on. Multiplying two elements of the ring $a(x)*b(x)$, we get the element $c(x)=c_0+c_1x+\cdots++c_{n-1}x^{n-1}$, in which the coefficient c_k is calculated by formula 1. Such a ring is called the ring of truncated polynomials. [4]

$$c_k = a_0b_k + a_1b_{k-1} + \cdots + a_kb_0 + a_{k+1}b_{N-1} + a_kb_{N-2} + \cdots + a_{N-1}b_{k+1} \quad (1)$$

Description of the message transfer scheme:

1. N, q and p are predefined parameters;
2. Generating a public / private key pair. To generate keys, customers select two "small" polynomials f and g from the ring of truncated polynomials. The private key is a pair (f, f_p), and the public key h is calculated by the formula 2. The public key is sent to the server;

$$h = (pf_q * g) \bmod q \quad (2)$$

3. Before sending messages, clients through the server receive each other's public keys and exchange messages to establish a peer-to-peer connection via WebRTC. To reduce the load on the server, peer-to-peer connection installation messages are transmitted via the WebSocket protocol;
4. The first client converts the message m to the polynomial $M(x) \in L_m$. Then the "blinding" polynomial $r(x) \in L_r$ is selected and using the public key of the second client it calculates the ciphertext using formula 3. The polynomial $C(x)$ will be the ciphertext;

$$C(x) = p * r(x) * h(x) + M(x) \bmod q \quad (3)$$

5. The second client receives $C(x)$ and, using its private key, restores the original message M using formulas 4, 5 and 6 .. Then it computes. Then. The second client restores the original message M .

$$a(x) = r(x) * p * g(x) + f(x) * M(x) \bmod q \quad (4)$$

$$b(x) = f(x) * M(x) \bmod p \quad (5)$$

$$f(x) * b(x) * f_p(x) = M \quad (6)$$

Table 1. – JavaScript encryption speed measurements NTRUEncrypt

Characters	Time, s
200	2,1
500	2,6
1000	3,3

End-to-end encryption in the peer-to-peer network will avoid the problem of intercepting the data being sent. Also, this application should work in the browser so that the user does not have to install anything.

In connection with the requirements to install peer-to-peer connections between clients using WebRTC:

WebRTC is an open source project designed to transfer streaming data between browsers or other applications supporting it using peer-to-peer technology. [3]

Technology benefits:

1. Conducting a conference in a browser greatly simplifies the process of holding a conference — the user does not need to install separate applications for this;
2. Used codecs provide good quality of communication;
3. The ability to implement any interface elements using HTML5 and JavaScript;
4. Open source gives you more options.

Technology flaws:

The technology defines only the general standard of data transmission (video and sound), but individual solutions of different browsers regarding the addressing of subscribers and other control processes are not compatible with each other. Therefore, even calls between a pair of different browsers present a separate complexity.

Establish a peer-to-peer connection between two clients (Figure 1).

A simplified connection scheme between two clients:

1. The first client sends Offer to the second client through the server;
2. The second client sends a response through the server to the first client;
3. A peer-to-peer connection is established between clients.

For quick transfer of messages to the server, the WebSocket protocol is used. WebSocket is a full-duplex protocol over TCP connection designed for real-time messaging between a browser and a web server. [5] Compared to HTTP, WebSocket sends much less service information with each request.

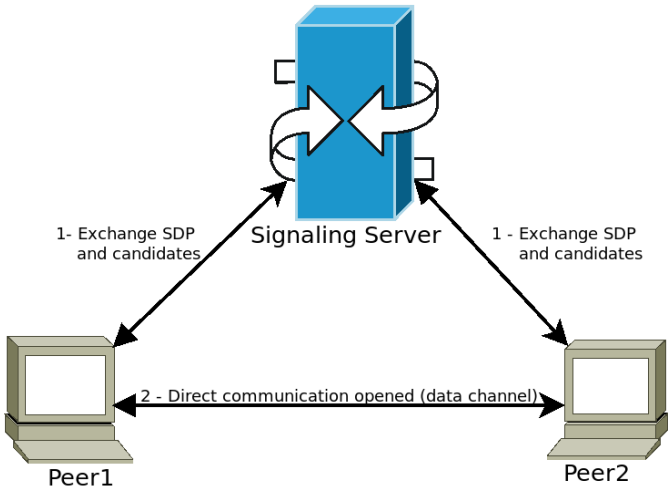

Figure 1. – Peer-to-peer connection between two clients

Conclusion. In the course of this study, a scheme for secure data transfer between users using a post-quantum encryption algorithm in a peer-to-peer network was designed. WebRTC was used to establish a peer-to-peer connection in the browser. For encryption, the NTRUEncrypt algorithm was used. It should be noted that the developed scheme leaves the opportunity for revision and introduction of additional protective equipment.

REFERENCES

1. Материал из Википедии – свободной энциклопедии. Одноранговая сеть [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/Одноранговая_сеть. Дата доступа: 20.09.2019.
2. Бутакова Н.Г., Семененко В.А., Федоров Н.В. Криптографическая защита информации: учебное пособие для вузов.- М.:Изд-во МГИУ, 2011. С 91–102
3. Материал из Википедии – свободной энциклопедии. WebRTC [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/WebRTC. Дата доступа: 20.09.2019.
4. Материал из Википедии — свободной энциклопедии. NTRUEncrypt [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/NTRUEncrypt. Дата доступа: 20.09.2019.
5. Материал из Википедии — свободной энциклопедии. WebSocket [Электронный ресурс]. Режим доступа: https://ru.wikipedia.org/wiki/WebSocket. Дата доступа: 20.09.2019.