Asymmetric Cryptosystems

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *Asymmetric cryptosystems are based on the complexity of solving the following three basic problems of mathematics [2-5]:1. Divide an integer that is large enough into prime factors. 2. Discrete logarithm in a finite field. 3. Calculate the roots of a system of linear algebraic equations in a finite area. The solution of each of these problems leads to problems that are complex and difficult, or theoretically proven to be unsolvable, even when today's computing devices are fully utilized.*

Keywords: U. Diffie and M.Ye. Hellman, RSA, EL-Gamal, electronic digital signature The encryption key is known to all, and encryption systems with a secret decryption key are called asymmetric cryptosystems, and such a public key cryptosystem was first developed in 1976 by U. Diffie and M.Ye.

INTRODUCTION

1. Asymmetric cryptosystems and their applications.

2. Asymmetric encryption algorithms.

3. Electronic digital signature.

Published in Hellman's "A New Direction in Cryptography" [1]. This article has raised the bar of open research in this field to a very high level. In this work, they created a scientific and practical method of encrypting and decrypting data in secret communication systems that does not require the transmission and reception of a secret key among system users through specially protected communication networks, which is still evolving and relevant today. non-confidential) ushered in the era of key cryptography.

Asymmetric cryptosystems are based on the complexity of solving the following three basic problems of mathematics [2-5]:

1. Divide an integer that is large enough into prime factors.

2. Discrete logarithm in a finite field.

3. Calculate the roots of a system of linear algebraic equations in a finite area.

The solution of each of these problems leads to problems that are complex and difficult, or theoretically proven to be impossible to solve at all, even when using the full capabilities of today's computing devices.

METHODS

For the purposes of this manual, the classic asymmetric cryptosystems include:

- RSA;

- EL-Gamal;

- Williams;

- abinRabin;

- Polig-Hellman;

- akMak-Alice

public key encryption algorithms, the mathematical elements based on them, and RSA, EL-Gamal electronic digital signature algorithms are considered and applied to specific issues.

To this end, we will first consider the necessary mathematical concepts and important properties associated with the above algorithms.

One of the main constituent elements of asymmetric cryptosystems is the use of sufficiently large (150 and more digit) prime numbers. .

Asymmetric key cryptosystems use two keys to exchange information. Two different asymmetric keys are mathematically connected. If one of them serves to encrypt the message,

the other is for decryption. These are called the user's public and private keys. The public key is public and the private key is public. Public keys are the same for everyone. Always convenient for contacts8.

Even if someone finds another user’s public key, they should not find the private key. This means that the intruder who finds the user's public key cannot find his private key mathematically. But finding a private key can be a big problem. Therefore, the owner of the key must keep his private key from various devices1.

If user A encrypts the data with his private key, the recipient must have user A's public key to decrypt the data. Recipient A must be able to decrypt user's message and decrypt it. Encryption and decryption with the same key is not possible when asymmetric key encryption technology is running1.

Encryption using a private key is not without its drawbacks. First of all, symmetric encryption does not solve the authentication problem. For example, Ali (A) may write a letter to Soli (S) but may not acknowledge that the letter was written by Wali (V). In addition, the symmetric key must be installed on the sending and receiving computers before sending the message. Of course, encryption for secure communication on the Internet makes sense when correspondents do not have to meet in person. The problem occurs when transmitting a secret key. True at, if the sender Ali passes the key to the receiving Governor without encryption, they can seize the key. If the key is sent in encrypted form, the receiving Governor cannot open it. To communicate with multiple correspondents, you must have separate keys for each recipient, which can be inconvenient. To solve this problem, an asymmetric encryption (public (public) key encryption) scheme has been proposed.

In algorithms called open-key encryption or asymmetric encryption algorithms, the key used for encryption is different from the key used to decrypt. Also, knowing the encryption key, it will not be possible to calculate the key required to decrypt it in a very long time. Any user can encrypt a message using an encryption key, but only someone with a decryption key that matches that key can read that message. The encryption key is called the public (public) key, and the decryption key is called the private (secret, private) key. The message can be encrypted using a private or public key, and recovery can be done using a second key. That is, text encrypted using a private key can only be retrieved using a public key, and vice versa. The private key is known only to the owner, and it is not given to anyone, and the public key is publicly distributed and can be made public. The two keys can be used to solve the authentication problem and to ensure confidentiality.

If the first key is closed, then it is used as an electronic signature, which allows you to authenticate the information, that is, to ensure the integrity of the information.

Common encryption algorithms. Cryptographic information protection standards, hash function. AYES [encryption standard (AES))] is a U.S. data encryption standard used for symmetric encryption. Block size 128 bits, key length 128,

8 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013

The base block, which consists of 192 or 256 bits, is based on an encryption algorithm. It has been in use since 20029. The DES [data encryption standard] is an American standard encryption system designed for use in symmetric encryption systems. It operated from 1977 to 1997 as the first open official standard of encryption in the world. It is based on a basic block encryption algorithm with a block size of 64 bits and a key length of 56 bits. It has 4 modes of encryption and 2 modes of code generation that authenticates the message10. The main areas of application of the DES algorithm:

1) storage of data on the computer (password and encryption of files);

2) message authentication (having a message and control group, it is not difficult to verify the authenticity of the message);

3) in electronic payment systems (transactions between a large number of customers and banks);

4) in the electronic exchange of commercial messages (protected from changes and interruptions in the exchange of information between the buyer, seller and the bank employee).

GOST 28147-89 Encryption Standard is a Russian encryption standard designed for use in symmetric encryption systems. It is based on a basic block encryption algorithm with a block size of 56 bits and a key length of 256, 512 bits. It has 4 modes of encryption.

The most common of the many different public key cryptosystems is the RSA cryptosystem, which was invented in 1977 and is named after its authors, Ron Rivest, Ada Shamir, and Leonard Heidelman. They took advantage of the fact that large prime numbers were simple to calculate, and that it was very difficult, if not impossible, to divide a number that is a product of two large numbers into multipliers. Deciphering the RSA cipher is equivalent to dividing by such multipliers (Rabin's theorem). Therefore, regardless of the length of the key, it is possible to estimate the lower limit of the steps required to decrypt, and to determine the time required to decrypt, knowing the speed of modern computers. The ability to determine the security assurance of the RSA algorithm is one of the reasons why it is popular among other public key algorithms. Therefore, the RSA algorithm is used in banking computer systems, especially when working with long-distance customers (credit card servicing).

The message hash function is a function whose value depends on each bit of the input sequence, that is, on each bit of the hash number given in the binary number system, or on each symbol of the hash source text10. The hashing algorithm returns a result of the same length from the input text. By length, we mean the number of bits in an expression given in the binary number system. For example, if the input text is an "ICT dictionary" and the hash function value is 10110111010100101, the hash function value is 17 bits long. There are also hash functions with output lengths of 128, 192, 256 bits. For the hash function to be effective, the result for the incoming message must be unique. Typically, hash functions are one-way functions. This is because it is very difficult to calculate the original text based on the output value. Hash functions are used to protect the security of data transmission and storage. 5. Electronic digital signature and public key structure. The purpose of using an electronic digital signature is, firstly, to confirm that the information in the electronic document is the original, and secondly, to prove to a third party (arbitrator, court, etc.) that the author of the document is this person. This to achieve the goal, the author must perform the process of "electronic signing" of the document in the prescribed manner with his secret individual number (individual key, password). In such a signature, each time the private key interferes with the information in the electronic document in accordance with certain rules. The number formed as a result of such an attachment (a sequence of numbers of a certain length) is an electronic digital signature of the author on this document. Thus, one of the two keys used in each of the digital signature and verification procedures is used. However, it must be ensured that it is not possible to identify the signature key using the verification key. The methods currently proposed involve the need for lengthy, complex computations to reset the signature key (private key) and the verification key (public key).

The idea of an electronic signature was first proposed in Diffie and Hellman's work to determine if the document was original and signed by the author.

Digital signatures are now widely used (a number attached to encrypted text that is transmitted or stored, which guarantees the integrity of the information and the authenticity of the author). Digital signature models based on symmetric encryption algorithms are also available.

RESULTS

The message hash function is a function whose value depends on each bit of the input sequence, that is, on each bit of the hash number given in the binary number system, or on each symbol of the hash source text10. The hashing algorithm returns a result of the same length from the input text. By length, we mean the number of bits in an expression given in the binary number system. For example, if the input text is an "ICT dictionary" and the hash function value is 10110111010100101, the hash function value is 17 bits long. There are also hash functions with output lengths of 128, 192, 256 bits. For the hash function to be effective, the result for the incoming message must be unique. Typically, hash functions are one-way functions. This is because it is very

9 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013

10 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.

difficult to calculate the original text based on the output value. Hash functions are used to protect the security of data transmission and storage. 5. Electronic digital signature and public key structure. The purpose of using an electronic digital signature is, firstly, to confirm that the information in the electronic document is the original, and secondly, to prove to a third party (arbitrator, court, etc.) that the author of the document is this person. This

9 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013

10 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.

DISCUSSION

Encryption using a private key is not without its drawbacks. First of all, symmetric encryption does not solve the authentication problem. For example, Ali (A) may write a letter to Soli (S) but may not acknowledge that the letter was written by Wali (V). In addition, the symmetric key must be installed on the sending and receiving computers before sending the message. Of course, encryption for secure communication on the Internet makes sense when correspondents do not have to meet in person. The problem occurs when transmitting a secret key. True at, if the sender Ali passes the key to the receiving Governor without encryption, they can seize the key. If the key is sent in encrypted form, the receiving Governor cannot open it. To communicate with multiple correspondents, you must have separate keys for each recipient, which can be inconvenient. To solve this problem, an asymmetric encryption (public (public) key encryption) scheme has been proposed.

CONCLUSION

In algorithms called open-key encryption or asymmetric encryption algorithms, the key used for encryption is different from the key used to decrypt. Also, knowing the encryption key, it will not be possible to calculate the key required to decrypt it in a very long time. Any user can encrypt a message using an encryption key, but only someone with a decryption key that matches that key can read that message. The encryption key is called the public (public) key, and the decryption key is called the private (secret, private) key. The message can be encrypted using a private or public key, and recovery can be done using a second key. That is, text encrypted using a private key can only be retrieved using a public key, and vice versa. The private key is known only to the owner, and it is not given to anyone, and the public key is publicly distributed and can be made public. The two keys can be used to solve the authentication problem and to ensure confidentiality.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

3 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

4Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

5 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

6 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

7 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013

8 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013

9 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013

10 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.