International Journal of Academic and Applied Research (IJAAR)
ISSN: 2643-9603
Vol. 5 Issue 1, January - 2021, Pages: 36-40

Fundamentals of Symmetric Cryptosystem

Usmonov Makhsud

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

Abstract: *Symmetric Encryption Algorithms - The key used to encrypt messages is derived from the decryption key, and vice versa, such cryptographic algorithms are called symmetric. Most symmetric algorithms use a single key. Such algorithms are called single-key or secret-key algorithms and require the sender and receiver of the message to agree on which key to use. The reliability of single-key algorithms is determined by key selection. If the perpetrator knows the key, it will be possible to decrypt all seized data without any resistance. This means that the selected key must be kept secret from strangers.*

Keywords: Encryption tables, Trisemuss cipher, Player cipher, binary square, bigram concept, AES, DES, GOST 28147-89.

INTRODUCTION

1. Symmetric encryption algorithms.

2. Bigram cipher of Trisemuss and Player.

3. Winston's 'double square' cipher

4. Modern symmetric encryption algorithms

Symmetric Encryption Algorithms - The key used to encrypt messages is derived from the decryption key, and vice versa, such cryptographic algorithms are called symmetric. Most symmetric algorithms use a single key. Such algorithms are called single-key or secret-key algorithms and require the sender and receiver of the message to agree on which key to use. The reliability of single-key algorithms is determined by key selection. If the perpetrator knows the key, it will be possible to decrypt all seized data without any resistance. This means that the selected key must be kept secret from strangers.

METHODS

There are two types of symmetric encryption algorithms. One of them handles bits of plain text. These are called streaming algorithms or streaming ciphers. In the second, the plaintext is divided into blocks of several bits. Such algorithms are called block algorithms or block ciphers. In modern computer algorithms of block encryption, the block length is usually 64 bits. Symmetrical systems have the following two problems:

1) How can participants in the exchange of information pass the secret key to each other?

2) How to determine the authenticity of the message sent?

Example of a symmetric key encryption scheme in the following example

we go out Correspondents named Ali (A) and Wali (V) want to exchange messages with each other. Each correspondent has its own secret key, which they can use to encrypt data before sending a message over the network. To illustrate the encryption scheme more clearly, we describe the key as a simple key and the encrypted message as an envelope. The encryption and decryption process is illustrated in the following figure.

Figure 7.1. Encryption system using symmetric key

User A encrypts the message with his private key and sends the message over the network, while recipient V (using the same secret key) retrieves the message. The figure shows the symmetry of the scheme. Users on the left and right use the same (symmetric) keys, so this type of encryption is called symmetric key encryption.

Symmetric cryptography is used in cryptosystems. The sender and receiver use two identical keys, incryption and decryption. The switches have two functions. These can be observation or control of incryption and decryption.

Symmetric keys are also called secret keys. Because they are based on privacy and protection from the user. He could decrypt the message if he had the keys. The symmetric incryption key Each pair of data sharing users must have two identical pattern keys. This means that if A and B want to share information, they must both have the same key. If you want to communicate with A- B and C in the same way, they should have two identical keys in their bar. This will reduce the chances of communicating with hundreds of friends in a short time. Keeping the right keys for the right person can be a daunting task6.

If 10 people want to communicate with each other in secret, each of them will need 45 keys. If that's 100 people, that's 4,950. These numbers can be found by the following formula1.

$N = n * (n-1) / 2.$

Traditional (classical) encryption methods include replacement ciphers, simple and complex exchange ciphers, and their combinations and modifications. It should be noted that there is a combination of replacement ciphers and replacement ciphers various types of symmetric ciphers used in memory.

In replacement ciphers, the letters of the encrypted text are replaced within that block of text according to certain rules. Replacement ciphers are the simplest and oldest. Encryption tables. At the beginning of the Renaissance (late 14th century), cipher tables were used in replacement ciphers. The keys to encrypted tables are: table size; a word or phrase denoting a substitution; property of the table structure

Trisemuss encryption tables. 1508 German abbot Johann Trisemuss

He wrote a book called Polygraphy. For the first time in this book, he systematically explained the use of alphabetical encryption tables. To obtain such a cipher, tables were used to write the letters of the alphabet and the keyword (or phrase). The keyword is entered in the table in a row, leaving out the repetitive letters. This table is then filled in with the missing letters of the alphabet. Because of the ease of remembering a keyword or phrase, such an approach would simplify the encryption and decryption process. [15] Let's look at this encryption as an example. For the Latin alphabet, we take the table size to be 6x5. The key word is ANZURA. If the letters are repeated in the keyword, the keyword will appear ANZUR because the next repeating letter is omitted. We start placing the letters of the keyword ANZUR from the first row, the first cell of the table.

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

If the first line is full, continue placing the letters from the second line. Once the keyword is entered, we start placing the letters of the alphabet in the table from the beginning. If the letter of the alphabet is present in the keyword, it is omitted and the placement of the next letter is continued. When the row is full, the placement starts from the next row. In encryption, the next letter of plaintext is found in this table, and the letter at the bottom of this column is written as the letter of the cipher. If the text letter is in the bottom row, the top letter of that column is taken for the ciphertext.

For example, if we encrypt the following message using this table:

WE ARE A TEAM

We get the following ciphertext:

WPE WPG ECVWCVPE

To decrypt this ciphertext, the next letter of the ciphertext is found in the table, and the letter at the top of this column is written as the text letter. If the letter of the text is in the top row, the bottom letter of this column is taken for the text.

If the text is decoded:

WE ARE A TEAM

Such encryption tables are called multi-gram because they are encrypted with a single letter. Trisemuss was one of the first to learn that encryption tables can encrypt in two letters. Such encryption is called bigram encryption.

The bigram cipher of the player. Player cipher was invented in 1854 and is the most famous bigram of the exchange. It was used in Great Britain during the First World War. At the heart of the player's cipher lies a table of encrypted letters of the alphabet that are roughly located in the primary message. [15] For ease of remembering the table encrypted by the sender and receiver of the message, a keyword (or phrase) can be used to fill in the initial rows of the table. In general, the structure of the Player encryption table is similar to the Trisemuss encryption tables. Therefore, in order to understand the encryption and decryption procedures, we use the Trisemuss encryption table discussed earlier in the Player system:

The encryption procedure includes the following steps:

1. The given message is divided into open text pairs (bigrams). The text should consist of an even number of letters and should not contain a bigram of two identical letters. If these conditions are not met, the text will be changed despite some spelling errors.

2. Open-text sequential bigrams are encrypted using the following encryption tables

According to the rules, the cipher is transferred to the text bigrams:

a. If both letters of a plaintext bigram are not arranged in a row or column (such as the letters A and F in the table above), a rectangular letter is found for the pair of letters to be identified. (In our example, these AF CU letters are represented by a pair of AF letters in the CU pair. The sequence of letters in the ciphertext is a clear text bigram.

should be located in a mirror relationship).

b. If plain text bigram letters are placed in one column of the table, then the letters at the bottom of them are taken as ciphertext letters. (For example, the NJ bigramma provides the DQ ciphertext). If the plaintext letter is in the bottom line, then the letter in the top line of this column is taken for the ciphertext. (For example, IZ bigramma OX shifrmatn bigr aunt).

c. If the bigram of the plaintext has both letters on the same line, then the letters to the right of them are taken as the letters of the ciphertext. (For example, the CV bigram provides a UW ciphertext text bigram). If the plaintext letter is in the far right column, the letter in the left column of the same line is taken for the cipher. (for example, the UP bigram gives the TA ciphertext bigram). When decrypting, the actions are performed in reverse order. It should be noted that encryption by bigrams quickly increases the durability of ciphers.

Winston's 'double square' cipher

In 1854, Charles Winston of England invented a new method of encrypting bigrams, thus contributing to the development of cryptography. It is called a 'double square' because it resembles a polyban cipher. Winston cipher opened a new stage in the history of cryptography. Unlike the polybian cipher, the 'double square' encryption method used two tables. These tables are horizontal, and the encryption is encrypted by bigrams, such as the Pleiphor cipher. Manual encryption with uncomplicated modifications has become very convenient, giving birth to a new reliable cryptographic system in cryptography. This method

Because of its reliability, it was used in Germany and even in World War II. [15] To encrypt the information, two tables with arbitrary letters of the Cyrillic alphabet were obtained.

To encrypt, the text is divided into pairs of letters, ie bigrams. Each bigram is encrypted separately. The first table on the left was used for the first letter of each pair, and the second table on the right was used for the second letter. In encryption, the first letter of the pair is taken from the left table, and the second letter is taken from the right table. To get the letters of the cipher, the text finds the first letter in the left table, the second in the right table, and then creates an imaginary rectangle with the corners of these letters so that they stand in the corners. The letters in the other corners of this rectangle represent the cipher bigram. Suppose that the IL bigram of a given text is encrypted. The letter I is in the first, column 1 and row 2 of the left table. The letter L is in column 5 and row 4 of the table. This rectangle consists of rows 2 and 4, as well as columns 1 of the left table and 5 of the right table.

Thus, the ciphertext bigram includes the letter O in the right column 5 and row 2 of the table, and the letter V in column 1 and 4 of the left table. Thus we obtain the OV ciphertext bigram for the IL bigram of the given text.

If both letters of the bigram are on the same line, then the letters of the cipher are also taken from the same line. The first letter of the code bigram is taken from the left table, the letter corresponding to the second letter column of the message bigram. The second is the letter from the right table corresponding to the column where the first letter of the message bigram is located. Therefore, the TO bigram becomes the DB ciphertext bigram. In the same way, message bigrams are encrypted. For example. Encrypt the message below:

WINSTON'S DOUBLE SQUARE CODE

APPLIED MATHEMATICS AND INFORMATICS

Divide the given message into bigrams (mark _ for the space):

UI NS TO NN IN G_ IK KI LA NG AN _K VA DR AT _Sh IF RI

AM AL IY-M AT EM AT IK A- VA –I NF OR MA TI KA

If we use Wheatstone's 'double square' cipher for the given message, we get the following bigram ciphertext.

'N GF JB GU: DL JZ' R FO GN UD: Sh :: NM shch_ XJ TJ

Combining a large-scale cipher gives the following simple cipher:

'NGFJBGU: DLJZ'RFOGNUD: Sh :: NMshch_XJTJ

When decrypting, the actions are performed in reverse order. If we use Wheatstone's "double square" cipher for the Cyrillic alphabet, the number of selected table cells should be 35. Because it also includes punctuation, such as periods, commas, and colons. The record line must be at least 30, which makes it very difficult to open. The 'double square' method encryption is very durable and simple to use.

Common encryption algorithms. Cryptographic information protection standards, hash function.

AYES [encryption standard (AES))] is a U.S. data encryption standard used for symmetric encryption. It is based on a basic block encryption algorithm with a block size of 128 bits and a key length of 128, 192 or 256 bits. It has been in use since 20027.

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. 4 modes of encryption and message authenticity has 2 modes of code generation7.

The main areas of application of the DES algorithm:

computer data storage (password and file encryption);

message authentication (having a message and control group makes it easy to verify the authenticity of the message);

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

in the electronic exchange of commercial messages (between the buyer, the seller and the bank clerk)

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

protected from making and retaining changes in data exchange).

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.

RESULTS

Because of its reliability, it was used in Germany and even in World War II. [15] To encrypt the information, two tables with arbitrary letters of the Cyrillic alphabet were obtained.

To encrypt, the text is divided into pairs of letters, ie bigrams. Each bigram is encrypted separately. The first table on the left was used for the first letter of each pair, and the second table on the right was used for the second letter. In encryption, the first letter of

the pair is taken from the left table, and the second letter is taken from the right table. To get the letters of the cipher, the text finds the first letter in the left table, the second in the right table, and then creates an imaginary rectangle with the corners of these letters so that they stand in the corners. The letters in the other corners of this rectangle represent the cipher bigram. Suppose that the IL bigram of a given text is encrypted. The letter I is in the first, column 1 and row 2 of the left table. The letter L is in column 5 and row 4 of the table. This rectangle consists of rows 2 and 4, as well as columns 1 of the left table and 5 of the right table.

Thus, the ciphertext bigram includes the letter O in the right column 5 and row 2 of the table, and the letter V in column 1 and 4 of the left table. Thus we obtain the OV ciphertext bigram for the IL bigram of the given text.

DISCUSSION

Symmetric cryptography is used in cryptosystems. The sender and receiver use two identical keys, incryption and decryption. The switches have two functions. These can be observation or control of incryption and decryption.

Symmetric keys are also called secret keys. Because they are based on privacy and protection from the user. He could decrypt the message if he had the keys. The symmetric incryption key Each pair of data sharing users must have two identical pattern keys. This means that if A and B want to share information, they must both have the same key. If you want to communicate with A- B and C in the same way, they should have two identical keys in their bar. This will reduce the chances of communicating with hundreds of friends in a short time. Keeping the right keys for the right person can be a daunting task6.

If 10 people want to communicate with each other in secret, each of them will need 45 keys. If that's 100 people, that's 4,950. These numbers can be found by the following formula1.

$N = n * (n-1) / 2.$

Traditional (classical) encryption methods include replacement ciphers, simple and complex exchange ciphers, and their combinations and modifications. It should be noted that there is a combination of replacement ciphers and replacement ciphers various types of symmetric ciphers used in memory.

CONCLUSION

In 1854, Charles Winston of England invented a new method of encrypting bigrams, thus contributing to the development of cryptography. It is called a 'double square' because it resembles a polyban cipher. Winston cipher opened a new stage in the history of cryptography. Unlike the polybian cipher, the ‘double square’ encryption method used two tables. These tables are horizontal, and the encryption is encrypted by bigrams, such as the Pleiphor cipher. Manual encryption with uncomplicated modifications has become very convenient, giving birth to a new reliable cryptographic system in cryptography. This method

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