Software Analytical Method for Protecting Digital Information

Baimuhamedov M.F., Zhikeyev A.A., Bulaev A.G., Tastemirova Zh.A., Kurmangalieva A.K., Bugubaeva A.U.

Abstract**:** ***Known to date means of information protection does not have a high degree of noise immunity and reliability. This work is related to the development of a more effective way to protect the source information using a software-analytical method based on the Vigenère cipher. The best known and most widely used methods of symmetric encryption are DES and the Vigenère cipher. The Vigenère cipher is a polyalphabetic encryption method for alphabetic text by using key words. The Vigenère cipher requires a single key asked a set b of letters. These sets are signed with the repetition of the message, and then the generated sequence is added back to the plaintext on modul (the power of the alphabet). To achieve this goal we propose to use multiple iteration in which the corresponding algorithms of encryption and decryption consist of successive cycles of the same type of encryption. The developed mathematical model for block coding, as well as methods and algorithms for their decoding. Presented in a modified Vigenère algorithm with the use of a block cipher based on variation of number of iteration with shift key, allows, in contrast to the known algorithms that more reliably protect the data on the Web server.***

Keywords**:** ***information security, algorithms, encryption, decryption, block coding, Vigenère cipher.***

I. INTRODUCTION

The modern development of human society requires processing and transmission continuously of the increasing volumes of various information. Due to the increase in requirements to efficiency of administrative processes, continuous growth of volume and information transmission rate, requirements and to reliability of the transmitted data significantly increased.

Revised Manuscript Received on June 30, 2020.
***** Correspondence Author

Baimuhamedov M. F.*, PhD in technical sciences, Z. Aldamzhar Kostanay Social and Technical University, Kostanay, Kazakhstan. Email: bmf45@mail.ru

Zhikeyev A.A., PhD in technical sciences, PhD in technical sciences, head of the Distant Learning Institute of A.Baitursynov Kostanay State University, Kostanay, Kazakhstan. Email*:* a_zhikeev@mail.ru

Bulaev A.G., PhD in biological sciences, Head of the Laboratory of Chemolithotrophic Microorganisms, Research Centre of Biotechnology RAS, Russian Federation. Email: bulaev.inmi@yandex.ru

Tastemirova Zh.A., Master of Economic Sciences, Senior Lecturer, Department of Economics and Finance, A.Baitursynov Kostanay State University, Kostanay, Kazakhstan. *Email:* azalia-zhanara@mail.ru

Kurmangalieva A.K., PhD in Economics, Associate Professor, Associate Professor, Department of Economics and Finance, A.Baitursynov Kostanay State University, Kostanay, Kazakhstan. *E-mail*: bektau@mail.ru

Bugubaeva A.U., PhD in Agricultural Sciences, Deputy Head of the Regional "Smart Center" of A.Baitursynov Kostanay State University, Kostanay, Kazakhstan. Email: alia-almaz@mail.ru

Treat the most known software and hardware tools of protection of the transmitted data and the files located on the third-party server:

- the hardware scramblers of a network traffic realizing algorithms (for example, DES) protective semantic conversions of the transmitted data with uniform secret key for encoding and decoding or algorithms (RSA, PGP, etc.) with couple of keys, one of which serves for encoding (public key), and another for decoding (secret personal key);
- complex gateway hardware-software protective screens, or "firewalls" (firewalls);
- filters of a network traffic on network (IP), transport (TCP, UDP) and application-oriented (FTP, Telnet, HTTP, SMTP, etc.) levels, information which are realizing also recording, excitation of alarm bells and encoding/decoding of information;
- hardware-software analyzers of a network traffic;
- the protected network OS and programming systems.

The industry of computer safety promptly develops. Many foreign firms develop original software and hardware tools of protection. There are certified network security features. For example, the Alf's Relcom company certified the firewall with the name "Pandora".

Nevertheless, means of information protection known so far don't possess a high level of noise immunity and reliability.

This article is connected to development of more effective method of protection of the initial information with use of the Vigenère cipher.

II. METHADOLOGY

A. Submission of the paper

For data encryption located on the server different cryptoalgorithms are used: pseudorandom number generator, DES algorithm, Vigenère cipher, RSA algorithm.

Effective methods of protection are based on classical cryptography of which use of one confidential unit - a key is characteristic. The used key allows the sender to encrypt the message, and to the receiver to decrypt it. In case of encryption of data storable on magnetic or other information media, the key allows to encrypt information in case of record on the carrier and to decrypt when reading from it.

The most known and widely used methods of the symmetric encoding are the algorithm of DES and the Vigenère cipher.

The Vigenère cipher - a method of polyalphabetic encoding of the alphabetic text with use of a keyword.

The algorithm of DES realizes encoding of 32, 64 or 128-bit data units by means of a key dimensionality from about to 2040 bits.

Decoding in DES is operation by reverse to encoding and is executed by repetition of operations of encoding in the return sequence. Process of encoding consists in initial swap of bits of the 64-bit unit, sixteen cycles of encoding and, at last, the return swap of bits.

It is necessary to mark that in case of the tables used when encoding, are standard, and, therefore, shall join in implementation of an algorithm in an invariable look.

The Vigenère cipher requires storage of one key set by a set from b of letters. Such sets are signed with repetition under the message, and, then, add the received sequence with clear text on module n (alphabet power).

Encoding is carried out according to expression:

$$V_{igr}(m_i) = (m_i + k_i \bmod d)(\bmod n)\,, \qquad (1)$$

decoding:

$$V_{igr}(m_i) = (m_i - k_i \bmod d)(\bmod n)\,. \qquad (2)$$

The Vigenère cipher as the simplest algorithm of the symmetric protection is the basis for the offered method of protection.

For achievement of a goal it is offered to use repeated iteration in case of which the appropriate encryption algorithms and decoding consist of serial same cycles of encoding.

We will use protection methods on the Vigenère algorithm and its modifications using security features without back coupling as use of a method *with* back coupling is impossible in case of origin of a circuit noise of communication because change of one bit in the encrypted message leads to an error of decoding of all message. It leads to the fact that in the given situation it is necessary to request all message repeatedly that carries to time expenditure and employment of communication link.

Use of block codes allows to carry out incomplete decoding for obtaining information on the file. It allows to reduce congestion of the server in case of a large number of the connected users. For saving this advantage, it is offered in case of modification of the Vigenère code, to use the principle of block coding. In case of value of the unit eight bits, compliance to its Vigenère cipher when using the alphabet follows dimensionality *of n=256*. The alphabet offered in table 1 it is possible to cipher any files irrespective of type and dimensionality. The first line of the table is the direct alphabet, all subsequent lines are shifted on one element. 1

Table-I: The Vigenère code for encoding of files

```
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.......253 254 255
1 2 3 4 5 б 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.......253 254 255 0
2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.......253 254 255 0 1
3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.......253 254 255 0 1 2
4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.......253 254 255 0 1 2 3
5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.......253 254 255 0 1 2 3 4
6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.......253 254 255 0 1 2 3 4 5
7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.......253 254 255 0 1 2 3 4 5 6
        ……………………………………………………………………
        ……………………………………………………………………
254 255 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.......253
255 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24.......253 254
```

For encoding set two parameters i - one byte of the ciphered file, *j* - one byte of encrypting key. One byte of the encrypted file is result of encoding.

```
crypt(i,j:byte):byte;
begin
if j< (256-1) then
crypt :=i+j
else
crypt: =j-(256-i)
end;
```

Decoding works similar to encoding - the byte of the open file is calculated.

```
decrypt(i,x:byte):byte;
begin
if x>(i-i) then
decrypt:=x-i
else
decrypt:=x+(256-i)
end;
```

Input data: byte of a key, byte of the encrypted file.

Output data: Byte of the open message.

According to table 1 it is easy to check that these expressions are fair for all sets value of byte.

However, this approach doesn't solve a problem of compliance of units of the open and encrypted message. So, for example, when encoding to the provided table 2:

Table-II: Example of encoding of the file

Key	1	21	31	41	51	61	31	1	21	31	41	51	61
Open file	121	145	0	18	35	43	0	0	9	15	5	6	3
Encrypted file	122	166	31	59	86	104	31	1	30	46	46	56	64

The problem of compliance of the encrypted and open file as use of identical bits in the open file allows to recover public key is visible. For elimination of it is offered to use a repeated iterative method when encoding and decoding. For increase in cryptofirmness the encrypting key displaces on the second and the subsequent steps of iteration. Offset is calculated on residual of a key from the previous iteration.

Rectilinear process of encoding decoding is represented the following sequence of steps.

The first step corresponds to table 2, and the new steps given in tables 3-5 are entered. In the entered encoding step as the open file the encrypted file from the previous step is used, and there is an offset of encrypting key at residual length on the previous step.

Table –III The second step of encoding

Key	31	1	21	31	41	51	61	31	1	21	31	41	51
Encrypted file of 1 step	122	166	31	59	86	104	31	1	30	16	46	56	64
Encrypted file	153	167	52	90	127	155	92	32	31	67	77	97	115

Table –IV: The third step of encoding

Key	61	31	1	21	31	41	51	61	31	1	21	31	41
Encrypted file 2 steps	153	1b7	52	90	127	155	92	32	31	67	77	97	115
Encrypted file	214	198	53	111	158	196	143	93	62	68	98	128	156

Table-V: The fourth step of encoding

Key	51	61	31	1	21	31	41	51	61	31	1	21	31
Encrypted file 3 steps	214	198	53	111	158	196	143	93	62	68	98	128	156
Encrypted file	9	3	82	112	179	227	184	144	123	99	99	149	187

Comparing of the data provided in tables 3, 4, 5 dataful, provided in table 2 shows that, since the second step, the problem of compliance of bytes in the open and encrypted files is fixed, it results in impossibility detection of private key by method of drive of a probable word. At the same time, since the fourth step, different bytes of the open file can give identical bytes of the encrypted file that complicates determination of private key by methods of the frequency analysis. For N - iterative encoding it is necessary to pass source file N of times. In case of rectilinear approach this is true, but at the same time the possibility of use of this algorithm for block encryption is lost. We will generalize a method on block encryption. Block cryptosystems break the text of the message into separate units and then realize conversion of these units with use of a key. For the organization of the block cipher the repeated pass of the source file on encoding by units on one byte, irrespective of remaining bytes in the file is replaceable. At the same time we will cipher each unit in several passes with use of different bytes of a key which line items are calculated. For receiving the expressions used in case of computation we accept initial offset, equal to zero that corresponds to the first step of encoding displayed in a figure 1. Using residual of a key, we calculate initial offset for the second step of encoding.

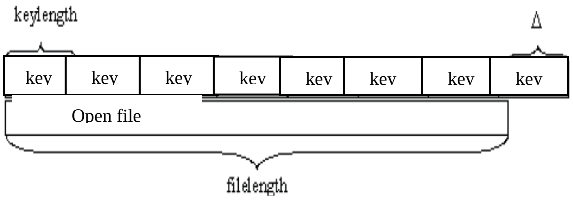

Fig. 1. Computation of offset for the second step of encoding

where

filelength - the number of bytes in the open file;

keylength - the number of bytes in encrypting key;

Δ - value of offset of a key on the second step of iteration.

Follows from the given designations that: $\Delta = filelength \bmod kekeylengt$.

Also shows that the residual of a key transferring to the following iteration identifies offset of encrypting key.

Computation of offset on any step is given in a figure 2 from which follows that computation of offset on any step of encoding is presented in the form.

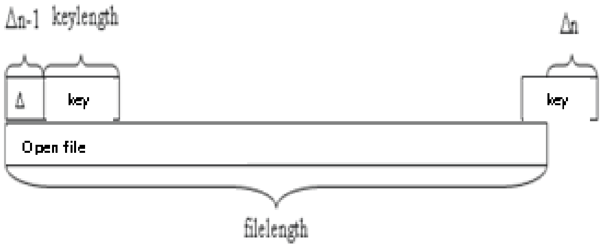

Fig. 2. General view of an algorithm of computation of offset:

$$\Delta_n = (filelength - (keylength - \Delta_{n-1}))\ mod\ keylength$$

where Δ_n - the calculated value of offset of a key on *n* step;

Figure 2. General view of an algorithm of computation of offset:

where

Δ_n - the calculated value of offset of a key on *n* step;

Δ_{n-1} - value of offset of a key on the previous step *(n-i)*

Follows from the aforesaid that it is long a key - there is a value indefinite, and in cases when

$\Delta=$ *fil elengthmod keylength =0*

That the second and the subsequent iterations didn't take place in empty, it is necessary to offset a key on T of bytes. Number T - the value set at the time of setting of a cryptosystem. Thus, the information security method offered by us using the Vigenère algorithm using block encryption based on variation of number of iteration with offset of a key provides more reliable data protection on Web - the server.

III. CONCLUSION

On the basis of the study of the existing methods of protection of transfer and storage of information and the most known software and hardware tools of information security by authors the effective method of protection of source codes of a software product and the files located on third-party Web - the server is offered. Mathematical models are developed for block coding of information and also methods and algorithms of their decoding. The modified Vigenère algorithm provided in article using block encryption based on variation of number of iteration with offset of a key allows, unlike the known algorithms, safely to protect data on Web - the server.

REFERENCES

1. A.P. Alferov. "Fundamentals of cryptography the manual" - A.Yu. Zubov, A.S. Kuzmin, A.V. Cheremushkin [Text]//the 2nd issuing corrected and dopopolnenny - M.: Helios of ARV, 2002. - 480 pages, illustrated,
2. S.P. Panasenko. "Encryption algorithms". Special reference manual [Text]//SPb.: BHV-St. Petersburg, 2009. - 576 pages: illustrated.
3. Thomas W. Cusick, Pantelimon Stanica. «Cryptographic Boolean Functions and Applications» [Text] // Academic Press is an imprint of Elsevier 525 B Street, Suite 1900, San Diego, CA 92101-4495, USA Linacre House, Jordan Hill, Oxford OX2 8DP, UK. First edition 2009.
4. A.Yu. Zubov, "Perfect ciphers": [Text]//M.: Helios APB 2003 1 illustrated.
5. Cryptography and encryption algorithms - [Digital resource]//[http://vse-shiiri.ru/.
6. Bruce Schneier. «Applied Cryptography» [Text] // Second Edition: Protocols, Algorthms, and Source Code in C (cloth), Publication Date: 01/01/96.

AUTHORS PROFILE

Baimuhamedov Malik Fayzulovich, PhD in technical sciences, professor, vice-rector for science and international affairs, Z. Aldamzhar Kostanay Social and Technical University.
Email: bmf45@mail.ru
Scientific work: 5 monographs, 7 textbooks, as well as over 140 titles of scientific papers were published;
Academic title, specialty: professor of Higher Attestation Commission.

A current member of the Dissertation Council D.05.11.034 at the Institute of Physical and Technical Problems of the National Academy of Sciences of the Kyrgyz Republic, a member of the editorial board of the All-Russian scientific journal "Agrarian Bulletin of the Urals", an editor-in-chief of the International scientific journal "Problems of Law and Economics",

Academician of the International Academy of Informatization (MAI) and the International Economic Academy of Eurasia (IEAE).

List of significant works: “Intellectualization of computer technologies for teaching.” (Monograph RIC, Alma-Ata, 1993, 276 pp.); “Expert Systems” (textbook, Kostanay Printing House, 2007, 212 p.); “Information Systems”, (textbook. MASTER REPRINT Publishing House, 2012, p.370) "INFORMATION SYSTEMS" (textbook (in English), Bastau Publishing House, Almaty, 2013 - p. 288).

Awards, titles: Badge "Honorary Worker of Education of the Republic of Kazakhstan", Badge "Excellence in Education of the Republic of Kazakhstan", diplomas of the Ministry of Education and Science of the Republic of Kazakhstan, regional and city akimats, diploma of the International Academy of Informatization.

Zhikeyev Azamat Aitpayevich, PhD in technical sciences, head of the Distant Learning Institute of A.Baitursynov Kostanay State University.
Email: a_zhikeev@mail.ru

Scientific work: since 2005, about 49 works were published in domestic and foreign scientific journals, including those approved by the Ministry of Education and Science of the Republic of Kazakhstan, and international ones with a non-zero impact factor;

Since 2016 - work in a group of performers in research projects on grant financing of the Ministry of Education and Science of the Republic of Kazakhstan, Ministry of Agriculture of the Republic of Kazakhstan.

Public work: a member of the disciplinary commission of A. Baitursynov KSU, Conciliation Commission, Scientific Council, administration, developer of normative and reference documentation of A. Baitursynov KSU.

Chairman of the Kostanay City Parental Public Council of the Education Department of the Akimat of Kostanay, member of the commission on minors and the protection of their rights under the Akimat of Kostanay, member of the political party “Nur Otan”.

Awards: Diploma of the Minister of Education and Science of the Republic of Kazakhstan, 2017; letter of rector of the university, 2016; Certificate of Akim, 2019.

Bulaev Alexander Genrikhovich, PhD in biological sciences (Microbiology), Head of the Laboratory of Chemolithotrophic Microorganisms, Federal State Institution «Federal Research Centre «Fundamentals of Biotechnology» of the Russian Academy of Sciences» (Research Centre of Biotechnology RAS).
Email: bulaev.inmi@yandex.ru

Scientific work: over 20 scientific publications were published in domestic and international respected scientific magazines, for the part of the inventions patents were obtained etc.

The work of the laboratory is supported by programs of the Presidium of the Russian Academy of Sciences, grants from the Russian Federal Property Fund, the President of the Russian Federation, and subsidies from the Ministry of Education and Science (as part of event 1.2). In the laboratory, more than 10 economic agreements were concluded with enterprises of the Russian Federation and the CIS to optimize and develop biohydrometallurgical technologies.

Tastemirova Zhanara Asylbekkyzy, Master of Economic Sciences, Senior Lecturer, Department of Economics and Finance, A.Baitursynov Kostanay State University.
Email: azalia-zhanara@mail.ru

Scientific work: More than 50 scientific publications, including those included in the RSCI database and in journals recommended by KKSON MES RK; Electronic textbooks in the amount of 2 of them 1 in the state language (Kazakh); 9 teaching materials and tutorials, including 2 in the state language, approved and recommended by the BMS of A. Baitursynov Kostanay State University.

Awards: 2 Certificates of the rector; Diploma of the dean; Certificate of the akim of Kostanay region “For many years of conscientious work and in honor of the Independence Day of the Republic of Kazakhstan”; Certificate of the Ministry of Education and Science of the Republic of Kazakhstan “Urmet literaty”.

Kurmangalieva Aizhan Kasymbekovna, PhD in Economics, Associate Professor, Associate Professor, Department of Economics and Finance, A.Baitursynov Kostanay State University.
E-mail: bektau@mail.ru

Scientific work: More than 80 scientific publications, including those included in the RSCI database and in journals recommended by KKSON MES RK; Electronic textbooks in the amount of 4 of them 2 in the state language (Kazakh); 11 teaching materials and tutorials, including 6 in the state language, approved and recommended by the Training and Methodological Council of A. Baitursynov Kostanay State University.

Awards: 2 Diplomas of the rector; Letter of thanks of the rector “For responsible performance of official duties, successes achieved in educational-methodical, scientific and educational activities, innovation in labor, excellent work”; Letter of thanks of the Ministry of Education and Science of the Republic of Kazakhstan.

Bugubayeva Aliya Uzbekovna, PhD in Agricultural Sciences, Deputy Head of the Regional “Smart-Center” of A.Baitursynov Kostanay State University.
Email: alia-almaz@mail.ru

Scientific work: number of publications - 43, of which: 1-monograph and 3 publications in a peer-reviewed foreign scientific publication indexed in the Web of Science or Scopus databases with non-zero impact factor;

Leading Researcher of Active Projects funded by the Ministry of Education and Science of the Republic of Kazakhstan;

Awards: Diploma for contribution to the development of agricultural science from KazAgroInnovation, 2011; Certificate for contribution to the development of Kostanay State University, 2018.

Further training: certificates "ISO / IEC 17025: 2017" General requirements for the competence of testing and calibration laboratories "; “Measurement and testing in shipbuilding and related industries”; "Office management at the enterprise"; "Systems of machine control software"; “Commercialization is a tool for integrating science and business”.