USING WEBPAGES AS CRYPTOGRAPHIC KEYS IN A ONE-TIME PAD SYSTEM

Farman MAMMADOV*, Elkhan SABZIEV**

*National Defence University, Military Scientific-Research Institute, Baku, Azerbaijan, **Azerbaijan National Academy of Sciences, Control Systems Institute, Baku, Azerbaijan

Nowadays, in order to ensure its confidentiality, it has become necessary to take additional measures during the transfer of information from one place to another through modern network technologies. In the symmetric encryption algorithms developed for this purpose, the sensitive aspect is the secrecy of the information used as a cryptographic key. In this paper, the problem of sending the key to the parties and the solutions proposed for this purpose were analyzed, and information about one-time pads and their features were provided. In this research, an approach for using web pages as a one-time cryptographic key is proposed. At the same time, a method of identifying and agreeing to use web pages and social network posts as cryptographic keys has been developed.

Key words: *cryptography, symmetric encryption, encryption algorithms, cryptographic key, one-time pad*

1. INTRODUCTION

Threats to the critical infrastructure of institutions responsible for the security system are real in every state. With the progress in data exchange the usage of information technologies for sending, storing and processing information in modern armies, as well as its spread to all the spheres of life has led to the strengthening of the interest of cyber attackers (criminals), and the unauthorized access and modification of information by third parties are increasing day by day.

Information security is data protection, processing, uninterrupted operation of complex infrastructures, combined by the joint application of various information and communication technologies, hardware and software, methods of combating other cyber threats, and various means of information protection.

Secure exchange of information is always important in organizing confidential communication.

A person who is serving in another country for the security interests of his country is needed reliable communication to protect himself and information from being intercepted, as well as sending relevant information to their home country and to continue his activities by receiving new missions.

Currently, the use of information technologies in various spheres, including unlimited access to the Internet anywhere in the world, opens up new prospects for the transfer of confidential information.

The info-communication industry offers various approaches to information security, and to the protection of information, containing confidential data, mainly within the interests of both the state and private sectors. During the exchange of information, containing confidential data, via electronic means, the main method of protecting it is the use of cryptographic products and solutions.

During cryptographic encryption, digital information, required for sending and protecting, is sent after being transformed into an incomprehensible form by means of an encryption algorithm and a specific key. The encryption algorithm is believed to be well-known, while decryption of encrypted information can be carried out by the use of a cryptographic key known only to the sending and receiving parties. That is why the crypto key plays a significant role in the exchange of confidential information, and symmetric encryption algorithms offer many approaches, algorithms, various methods, schemes, and solutions related to its creation, delivery to parties, storage, and modification of the crypto key.

The article analyzes the problem of sending a cryptographic key to the parties and the proposed solution methods for this purpose, as well as provides information on one-time pads and their features. The research paper proposes an approach for using web pages as a one-time cryptographic key. At the same time, a method of identifying and agreeing to use web pages and social network posts as cryptographic keys was developed.

2. PROBLEM OF SENDING A CRYPTOGRAPHIC KEY TO THE PARTIES

The most important parameter in ensuring reliable communication is the maximum level of protection of the cryptographic key and its secure delivery to the parties. In symmetric encryption methods, it is desirable to update the key regularly in order to increase the durability of the cryptosystem. In many cases, when there is a need to update the key, it is thought that its delivery to the

parties is the weakest point of the cryptosystem.

Various methods related to the topic were developed in the literature. As an example, the numbered form of rows and columns of the Polybius square (Gasimov: 2009, p.173), binary codes for image (Alqad: 2019; Shumay:2018), an agreed book (Gasimov:2009, p.189; Lele:2014; Ristanovic:2008), various files (Wang:2008; Wang:2010) and a memorized poem (Gasimov:2009, p.173) can be used as keys. The idea of using a web page as a cryptographic key is not provided in these and other methods, including classical steganographic methods (Aliguliyev:2006; Gasimov:2009, p.255). This part will cover some algorithms that can be applied during the exchange of a crypto-key.

In (Hussain:2008), S.M.Hussain və H.Al-Bahadili, using the key based random permutation (KBRP) method, proposed a new, efficient, functional, password-based algorithm that generates a key resistant to cryptanalysis. The KBRP method (Hussain:2008) provides the generation of a particular permutation of a given size ***N*** out of ***N*** permutations based on a given primary key. Here ***N*** indicates the required encryption key length. The algorithm consists of a computational stage in five steps – the first three spets involve the use of the KBRP method, and the next two steps involve the key generation and verification of cryptanalysis resistance.

So, in the first step, an array of ***N*** elements is compiled using the primary key. To do this, the ASCII values of the primary key are taken and stored in an array consecutively. If the length of the primary key is less than ***N*** starting from the value of the first element of the array, the missing massive elements are added consecutively and in pairs. At the completion of the first step, a summing operation modulo ***N+1*** is performed with each element so that the values of all elements of the array are numbers from 1 to ***N***.

The second step is to get rid of repeated values by replacing them with the value of "0" and keeping only one value out of these repeated values.

In the third step, the values "0" of the array are replaced with nonzero values in the range 1 to ***N***, which are not exist in the array. This completes the generation of a particular permutation of a given size ***N***.

At the fourth step, in order to convert the array values to "0" and "1", a modular operation with 2 is performed with them.

In the fifth step, in order to ensure that the number of "0" and "1" in the key is not equal, the extra bit is selected and replaced by another. To do this, 8 bits are taken from the key consecutively and the "0" and "1" contained in these 8 bits

are counted. If the numbers of "0" and "1" are equal, the bit at position 5 is replaced by another one. Thus, the key required for encryption is generated.

As already mentioned, the algorithm is based on the primary key, and key generation becomes possible only after that. In this case, there is a need for a preliminary agreement between the parties regarding the key or its preliminary sending to the parties.

In (Ghrare: 2018), S.E.Ghrare, H.A.Barghi və N.R.Madi propose a new encryption method based on a hidden encrypted symmetric key. While using this method, a key is generated based on the plaintext and is sent to the other party by hiding inside the cipher. Thus, this method also solves the problem of distributing the key to the opposite party. First, the plaintext is divided into two equal parts to generate a key. Then the first half is assigned to K_1, and the second half is assigned to K_1. One of the keys is encrypted through the other to get the final K key. The final key K is equal to half the length (number of symbols) of the plaintext. The user decides whether the K key will be generated based on K_1 or K_2. The plaintext is encrypted and hidden inside the key cipher by any of the steganographic methods. The other party first separates the key from the cipher using an agreed steganographic method and obtains the plaintext by performing a decryption operation. The encryption and decryption operation is performed according to the formulas (1) and (2):

$$C = E(K, M) = (M + K) \bmod 26, \quad (1)$$

$$M = D(K, C) = (M - K) \bmod 26. \quad (2)$$

Here, C – encrypted content sent, M – text of confidential information, E and D – encryption and decryption algorithms, respectively, K – cryptographic key, **26** – the number of letters in the English alphabet.

The method of S.E.Ghrare and others analyzed above provides the preparation of the plaintext key and sending it to the other party using steganography. The algorithm's main advantage is that each encryption operation is performed using a different and distinctive key. This can be classified into the class of one-time pads.

The approach proposed in (Pal: 2014) by S.Pal və P.Paul is based on the use of a human fingerprint in cryptography. Here, first, in a classical manner, the plaintext is encrypted with a certain key using the relevant algorithm. Then the biometric data of the sender's fingerprint is combined with the key. Finally, the ciphertext and the combined information of the key with the fingerprint are mixed and sent to the other party. During the decryption, the ciphertext and the key are separated from each other using fingerprint images stored in a

database of the receiving party, and decryption is performed on the basis of the relevant algorithm.

While using the algorithm, additional fingerprint-reading equipment is needed. At the same time, sending the primary key in combination with a fingerprint makes it necessary for the fingerprint of the person who encrypted the information to be available for the other party to perform decryption. If the fingerprint is not found in the relevant database or there is any problem with fingerprint reading, decryption becomes impossible. This can be considered the weakest point of the algorithm.

In (Akhila: 2016), V.A. Akhila, C.Arunvinodh, K.C. Reshmi and others present a new encryption method known as brain wave cryptography. The proposed approach is based on the use of brain waves or signals resulting from the human brain's neuron activity (nervous system) in generating an encryption key. Here it is said about generating a secret key, that can be used as a cryptographic key, from brain signals or developing a secret key with the help of brain waves. Due to the fact that brain waves have some of the most powerful biometric properties compared to other biometric means, the security of the key can be enhanced. The research paper also highlights the idea of solving the problem of the Online Brain Computer interface (BCI), as well as the idea that an independent component of interest (ICi) can be automatically selected by taking a certain area of the brain. During the generation of the encryption and decryption keys, a person is given some tasks on analyzing the brain signal. In this case signals from five parts of the brain (central, parietal, motor, occipital, and frontal) are seized by sensors and digitized. Then an independent component analysis (ICA) is used to independently suppress artifacts (artificial and extraneous signals) in the Electroencephalogram (EEG) recordings. ICA decomposes EEG signals into statistically independent components or sources and then is followed by the removal of artificial signals. After performing independent component analysis few components are selected as independent component of interest which is used for further processing. To take an average of frontal components of different EEG signals, a special procedure is repeated for all other parts of the brain (central, motor, parietal, occipital components) and is predefined as reference ICi. The obtained "ICi" is used while generating the encryption key.

With the help of the proposed approach, data storage security is ensured and implemented directly without using any medium for

the secret key. The decryption of information becomes possible only to those who encrypted it, and special equipment is needed.

In (Monrose: 2001), F.Monrose, M.K.Reiter and others propose a device that can generate a secure secret key using a primary password voiced by a person. In the proposed approach, the voiced primary password is first digitized. Then the obtained audio signals are sequentially divided into 10-millisecond parts and taken as 30-millisecond fragments. For each signal fragment, a frame of 12 units of power spectrum coefficients is determined. The frames of coefficients that contain pauses of silence at the start, middle, and end of the utterances are removed in order to achieve good results. The proposed approach uses an bit attribute descriptor to ensure specificity in case the same utterance is voiced by a relevant person. The attribute descriptor is obtained by dividing the frames of the coefficients into consecutive frames or segments. During key generation, frames or segments are stored in a database inside the device to determine the uniqueness of the primary password and the person who uttered it. Data storage in the database is carried out using the vector quantization method. During the vector quantization, clusters of vectors and parts are determined in a vector (in this case, a frame or segment) set of a given acoustic field. The central points of clusters are called centroids. The centroids are encoded in the database and the distances between them are stored. Each time the secret key is generated, the correspondence between the primary password and the addressing person is checked by matching with the information in the database. In the course of the research, 20 centroids were quantized for each person and the primary password. The device was tested with 250 passwords uttered by 50 users. Empirical evaluations show that the reliability and entropy (randomness and uncertainty) of the generated key can be high with the right chosen parameters. The created system has demonstrated resistance to cryptanalysis even when all the information used during generating and verifying the key, as well as the device was intercepted by attackers.

Special devices are used for encryption in a cryptosystem based on a primary password voiced by a person, and since it is performed depending on the person, its use for data protection is considered more appropriate.

In (Gupta: 2014), R R.Gupta və J.Anchal propose an algorithm for generating keys and encrypting images using DNA sequences. First, a special gene sequence of length ***4n*** is selected from the gene bank

in order to generate a cryptographic key. The start and end points of the sequence are chosen randomly. Then the chosen sequence is divided into substrings, and each substring is converted into a binary code using DNA coding. When coding DNA, it implies the participation of DNA bases (***A***- adenine, ***G*** - guanine, ***C*** - cytosine, ***T*** - thymine) in a paired form, where ***A*** and ***T*** are complementary, and ***G*** and ***C*** are complementary, as well as their denotation in the form of a binary number system (00, 01, 10, 11). Mathematically, if there is a total n number of substrings then the binary number generated from the DNA sequence is denoted as ***N***.

The next step is to expand the key. Elements of the key sequence are encoded into the DNA sequence using the DNA encoding method. The resulting DNA sequence is copied into substrings, then substrings are generated in each string. The first string is subdivided into the substrings of length ***4n*** and the division takes place from the first character. Similarly, the division of the second string takes place leaving the first character. The division is done with the third and fourth strings leaving the first two and first three characters. From all the strings only the substrings of length ***4n*** are chosen as the expanded key. For example, let the gene sequence selected from the gene bank to create a cryptographic key be ***ACT CCT GCT ACAT ATC***. In this case, the key extension will be like this:

ACTC/CTGC/TACA/TATC
A/CTCC/TGCT/ACAT/ATC
AC/TCCT/GCTA/CATA/TC
ACT/CCTG/CTAC/ATAT/C

Each substring is again denoted as a number. This completes the key expansion stage.

In the 3rd step, a pseudo random sequence is generated. If there are $M \times N$ pixels in the image to be encrypted then it is required to generate the pseudo random sequence of length MN. For this purpose, a 256-byte key, ***K*** and array ***S***, is chosen. The array ***S*** is filled with numbers from 0 to 255, i.e.

$$s[0] = 0, s[1] = 1, \dots, s[255] = 255$$

Now a 256-byte temporary array ***T*** is created and the values of ***K*** are copied into ***T*** and the remaining positions of ***T*** are filled again with the values of ***K***.

In order to generate the pseudo random sequence

$$Z = \{z[0], z[1], \dots, z[MN]\}$$

of length ***MN***, the following periodic operation is conducted:

$j = 0;$
$for\ i = 1\ to\ MN$
$for\ j = 0\ to\ 255$
$j = (j + s[i] + t[i])\ mod\ 255$
$z[i] = j\ mod\ 8$
$s[i] = s[j]$

In the last step, the encryption process is performed. Encryption is carried out in the Cipher Blok Chaining (CBC) mode. In CBC mode, randomly chosen 8–bit information is generated as a result of performing the ***XOR*** operation with bits with the first block of the plaintext and the first pixel values and is called the initialization vector (IV). At first, the pixel values of the original image are chosen as a matrix and converted into a one dimensional ***P*** sequence to be used for the encryption process. The following formula (3) is used to perform encryption.

The formula (4) below is used to perform the process of converting each value of sequence ***C*** into the DNA code.

where

$p_i \in P = \{p_0, p_1, p_2, \dots\dots\dots, p_{MN-1}\}$

– pixel values of the original image,

$k_i \in K = \{k_0, k_1, k_2, \dots\dots\dots, k_{n-1}\}$,

– key values,

$C = \{c_0, c_1, c_2, \dots\dots\dots, c_{MN-1}\}$

– the values of the original cipher, ***DnaAdd*** – function of the addition operation by the method of summing binary numbers, ***Comp*** – the function of checking binary numbers participation in the paired form while DNA encoding, ***Rotate*** – the function of rotating to the left in the direction of the DNA code, the number of bits rotated at iteration is equal to the value of the pseudo-random sequence.

This completes the encryption operation, and an sequence is generated.

During the decryption operation, the sequence is converted into a two dimensional matrix, and the image encrypted in the form of a DNA code is converted from binary to decimal pixel values.

3. ONE-TIME PADS IN CRYPTOGRAPHY

The use of one-time pads in computer systems is based on a device proposed in 1917 by Gilbert Vernam and patented (Elizabeth:1982, p.86; Smart:2004) during this period. Verman, an employee of the American Telephone and Telegraph Company, designed an encryption device based on the Baudot code and used in telegraphic communications.

$$c_i = \begin{cases} [IV \oplus p_0] \bmod 2^8, & i = 0 \\ [(c_{i-1} \oplus k_{i \bmod n}) \bmod 2^8], & 1 \le i < MN \end{cases} \quad (3)$$

$$x_i = \begin{cases} DnaAdd\left(c_1, Comp\left(Rotate(c_{MN})\right)\right), & i = 1 \\ DnaAdd\left(c_i, Comp\left(Rotate(x_{i-1})\right)\right), & 2 \le i \le MN \end{cases}$$

In the code Baudot each symbol is denoted as a combination of five marks and spaces, thus 32 symbols can be encoded. Each symbol of the encoded was collected in two modules with marks of the key.

The cryptographer of the US Army, Major Joseph Mauborgne, proposed the idea of applying the keys used in the device designed by G. Vernam only once (Gasimov:2009, p.86). By the use of these electrical signals, it was the first automated multi-digit substitution cipher in which the key length was equal to the length of the source text (Menezez: 2001, p.246). With this came the ideology of one-time pads, which never were broken.

Despite the existence of infinite computing resources of cryptosystems, including modern multicore computers, security is guaranteed perfectly, unconditionally or theoretically, when decryption is impossible. Despite how simple it may sound, the requirements for a cipher to be unconditionally secure are tremendous (Paar: 2010, p.36). The use of one-time pads in encryption is a great example. Keys, whose length is equal to the length of the text required to be encrypted, randomly generated, periodically non-recurring, non-guessable, as well as known only to the sender and recipient of information, are called one-time pads (Elizabeth:1982, p. 86). In cryptography, unconditional security can only be ensured by using one-time pads. In other cases, no encryption systems are considered completely secure (Menezes: 2001, pp.42-43).

One-time pads and running keys belong to non-periodic and streaming-encryption systems (Elizabeth: 1982, p.136) and are used in symmetric algorithms (Paar:2010, p.51).

The symbols (sometimes bits) in the key must be generated in a completely random sequence, the key must be known only to the parties involved in the transfer of information, the length of the key must be equal to the length of the plaintext, and each key must be used only once (Paar: 2010, p.37). One-time pads must be held by both parties and destroyed after each use.

The security of most cryptosystems is based on the generation of non-guessable values in algorithms. The random generation of these quantities or information bits is ideal in algorithms and protocols. It is impossible to simultaneously ensure the above-mentioned, as well as store one-time pads required to encrypt large amounts of information, manage them during intensive information exchange and transfer them to the parties without anyone's awareness.

Taking into consideration the complexity of the requirements for using keys only once, they are rarely used in practice (Paar: 2010, p.38). But in practice, one-time keys were widely used by Russian agents operating in foreign countries in the XX century (Menezes: 2001, p.47). After World War II, the security of the direct communication channel organized between Moscow and Washington during the Cold War was also ensured by the use of one-time pads (Menezes:2001, p.21).

As already mentioned, one-time pads were widely used by the Soviet Union during World War II. There was sometimes a lack of one-time pads due to the urgent demand for information sharing, and there were examples of keys being used two or more times because of an insufficient number of keys. As a result of the fact that the American and British counterintelligence kept all the lines of information sharing under control, and some keys were used more than once, secret Russian correspondence began to be uncovered. After this event in 1946, the Russians had to change their encryption system. Only 2,900 pieces totaling 5,000 pages out of the hundreds of Russian correspondences collected between 1941 and 1946, could be read during the next 25 years (Boneh:2015). The spread of Internet technologies in the modern era removes existing limitations on the development or generation of one-time pads.

4. PROPOSED APPROACH

In the method proposed in the article, the cryptographic key is located in a publicly available global Internet environment, and the web page to be used as the key is agreed in advance. It is proposed to take a cryptographic key from a certain section or part of the web page, which the parties agreed on in advance. Posts on social media pages might be used for the same purpose. The process for determining the web page or post in a social network to be used may be different. The website and the page of this website must be coordinated in order to use the web page as a key. For the same purpose, while coordinating social network pages, the social network, social network page, and post that will be used as a key must be determined.

The following sequence can be used to determine a web page. The parties specify the time when one of the sites with daily information postings is most frequently updated. Updating refers to the permanent publication of information on sites with a dynamic structure. Because every update of such sites leads to a new additional web page. That's why information sites and posts shared on social networks are more in line with this requirement. Thus, every day dozens of information are posted on information sites, which are displayed on a new web page. The table 1 shows the amount of information posted on some information sites in a day.

Table 1. Amount of added information in some web sites

Web site	Amount of added information
azertag.az	244
trend.az	140
report.az	252
day.az	174
moderator.az	155
apa.az	240
musavat.com	174
qafqazinfo.az	114
oxu.az	177
haqqin.az	102
ria.ru	350
lenta.ru	480

Table 1 provides information that the amount of data added daily to active sites in most cases exceeds a hundred. The amount of information on some sites is more than two hundred, and on some it is possible to post more than three hundred pieces of information. The amount of information posted on information sites varies from country to country depending on the political, economic, social, military, as well as regional and international situation. It is obvious that the frequency of adding webpages is not the same on all sites and does not always happen at the specified interval. Also, some active sites can only add one page per day. Anyway, it is not difficult to identify sites with a high frequency of updates.

According to electronic resources, the number of websites currently available on the Internet is over 1.13 billion. However, the number of active sites is only 18% of existing sites. It is reported that the number of sites created daily around the world is more than half a million or 250 thousand. 62.3% of existing websites provide information in English, 7.5% in Russian, and 3.8% in Turkish and Spanish. The Persian language is in next fifth place with 3.5% (Huss: 2023).

Given the frequency of updates, it is recommended to agree on which web page of the selected site and on which date information will be exchanged. So the approval process is predicted to be more memorable.

Various techniques can be applied in selecting a web page. For instance, it is possible to choose a cryptographic key from the data posted on the day of the exchange of information on a pre-agreed site. It is considered more memorable in a key approval process. To do this, we can agree that some information corresponding to this hour is taken as a key, taking into account the time when the most news is posted on the specified site. For example, a web page that posts one of the 1st, 2nd, 3rd, or other matched site news at a specified hour can be selected. It is

also possible to transfer information before the agreed time. In such a case, it can be agreed to take the news of the same hour a day earlier. If there is a need for more intensive, that is, more than one piece of information transfer during the day (that is, more than one piece of information is sent), then the specified news of the next hours or one of the subsequent news of the hour can be used as a cryptographic key. The web page to be agreed as the cryptographic key may be selected among the pieces of information posted on the site in previous periods. For example, one of the web pages where the information of the agreed hour posted one, two, three, etc. days ago can be retrieved and used. For the same purpose, it is possible to periodically set weekly, monthly, annual intervals.

The use of social network posts as a cryptographic key in the encryption of text-type data is slightly different from that of web pages in terms of their approval process. So, if posting information on sites increases the number of web pages, then text posts on social networks usually do not increase the number of web pages. However, it is possible to use text information posted in social networks as cryptographic keys in the method proposed in the research paper.

The agreement process for the use of social network posts as a cryptographic key includes the social network platform, the social network page and the publication on this page.

To agree on a cryptographic key from information posted on social networks, one of the open source pages on any social network must first be selected. Social network pages may be owned by individuals, corporate organizations, or official government agencies. It does not matter who owns the pages listed in the key selection.

The next component of agreeing a cryptographic key from social network pages is post-identification. The main difference and almost a disadvantage of choosing social networks as a cryptographic key from web pages is that their interface is made in the form of a news feed. In other words, there is no structured archive of social media posts. Therefore, it is not relevant to use old social network posts as a cryptographic key. Given this, it is recommended to use posts shared in social media within the last week as cryptographic keys for text encryption.

Once the website, web page of that site, as well as the social network page publication have been agreed upon, the next step is to determine which part of the text information or publication posted on the selected web page will be accepted as key. Text taken from a web page can be used as is. However, in this case, the resistance of the method to crypto-attacks may decrease. Therefore, it

is recommended that the whole text taken from a web page should not be used as a cryptographic key. To do this, it is suggested to use separate inconsistent paragraphs, sentences or words of text taken from a web page. For the same purpose algorithms can be used to mix paragraphs, sentences, or words. In accordance with one of these rules, it is necessary to agree on what part of the text extracted from the web page will be used as a cryptographic key.

Therefore, the web site, web page (or social network page, post), where cryptographic key will be taken to be used in the process of encryption, and the agreement prosedure of the text fragments taken from there is determined.

The method proposed in the article ensures that each cryptographic key is used only once. The proposed approach can be considered as corresponding to the ideology of single-use cryptographic keys. Thus, given the number of new web pages created daily in the world, it is possible to generate practically "infinite" keys from them and use them as single-use cryptographic keys. Moreover, such use of Internet pages, including web pages, as a cryptographic key combines several parameters of single-use keys. Although websites do not meet all the requirements for single-use keys, the availability of a wide range of keys allows them to be used for this purpose.

When web pages are implemented as cryptographic keys, the key becomes easier to be changed frequently and delivered to parties according to an agreed rule. Using the proposed method, it is possible to change the cryptographic key without any contact other than determining the agreement process between the parties involved in the information exchange. Given the power of the Internet, the new cryptographic key can be used as a real example of single-use keys.

When using web pages as a cryptographic key, the cryptographic key is equal to the length of the text, and has such properties as non-periodicity of repetition and impossibility to be decrypted.

Although each key can be used once when using web pages as a cryptographic key, it is not possible to destroy the key after each use or promptly after the retention period. The reason is that the web page used as a key is on servers located in different countries of the world.

The main advantages of encrypting web pages with cryptographic keys are as follows:

– the method is simple, since it does not require the construction of a complex mathematical model, as well as additional calculations;

– the cryptographic key to be used in encryption is determined only at the time of encryption;

– the cryptographic key used in the encryption process is used only once;

– no additional resources are required to store, manage and change the cryptographic key.

The proposed approach, together with other cryptographic methods, can be used to ensure the security of the confidential information.

5. CONCLUSIONS

The article deals with the use of web pages and social media posts available worldwide as cryptographic keys that can be easily used in symmetric encryption algorithms. It is shown that the possibility of using web pages as cryptographic keys, as well as social network posts, eliminates the problem of sending a cryptographic key to the parties with symmetric encryption and allows to change it frequently. The proposed approach can be easily applied in symmetric encryption methods to ensure information security.

ACKNOWLEDGEMENT

This article is original research and has not been published elsewhere.

REFERENCES

[1] Akhila, V.A., Arunvinodh, C., Reshmi, K.C., [et. al.], A New Cryptographic Key Generation Scheme Using Psychological Signals // *Procedia Technology*, 2016, 25, pp. 286 – 292.

[2] Aliguliyev, R.M., Imamverdiyev, Y.N., *Fundamentals of Cryptograpy,* Publishing House "Information technologies", Bakı, 2006, p. 688.

[3] Alqad, Z., Oraiqat, M., Almujafet, H. [et. al], A New Approach for Data Cryptography // *International Journal of Computer Science and Mobile Computing*, September 2019, Vol.8, Issue.9, pp. 30-48.

[4] Boneh, D., Shoup, V., *A Graduate Course in Applied Cryptography*, URL: https://crypto.stanford.edu/~dabo/cryptobook/draft_0_2.pdf

[5] Elizabeth, D., Denning, R., *Cryptography and data security*, USA and Canada: Addison-Wesley Publishing Company, Inc., 1982, 404 p.

[6] Gasimov, V.A., *Fundamentals of information security. Textbook*, MNS MTS Main Department Publishing Center, Baku, 2009, p. 340.

[7] Ghrare, S.E., Barghi, H.A., Madi, N.R., New Text Encryption Method Based on Hidden Encrypted Symmetric Key // *ACIT* 2018, Ceske Budejovice, Czech Republic, June 1-3, 2018, pp. 240-244.

[8] Gupta, R., Anchal, J., A New Image Encryption Algorithm based on DNA Approach // *International Journal of Computer Applications*, 2014, Volume 85, No 18, pp. 27-31.

[9] Huss, N. How Many Websites Are There in the World? (2023), URL: https://siteefy.com/how-many-websites-are-there/

[10] Hussain, S.M., Ajlouni, N.M., Key Based Random Permutation (KBRP) // *Journal of Computer Science*, 2006, 2 (5), pp. 419-421.

[11] Hussain, S.M., Al-Bahadili, H., A Password-Based Key Derivation Algorithm Using the KBRP Method

// *American Journal of Applied Sciences*, 2008, 5 (7), pp. 777-782.

[12] Lele, R., Jainani, R., Mikhelkar, V. [et. al.], The Book Cipher Optimised Method To Implement Encryption And Decryption // *International Journal Of Scientific & Technology Research,* 2014, Volume 3, Issue 1, pp. 11-14.

[13] Menezes, A.J., Oorschot, P.C., Vanstone, S.A., *Handbook of Applied Cryptography, Fifth Printing*, Boca Raton, USA: CRC Press, 2001, 816 p.

[14] Monrose, F., Reiter, M.K., Li, Q. [et al.], Cryptographic key generation from voice // *Proceedings 2001 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 2001, pp. 202-213.

[15] Paar, C., Pelzl, J., *Understanding Cryptography*, Berlin: Springer, 2010, 372 p.

[16] Pal, S., Paul, P. Cryptographic Technique Using Biometric Authentication // *International Journal of Innovative Research in Computer and Communication Engineering*, 2014, Vol. 2, Issue 9, September, pp. 5681-5685.

[17] Ristanovic, D., Protic, J., The Book Cipher Algorithm // *Dr. Dobb's Journal*, October, 2008, pp. 48-51. URL: drdobbs.com/security/the-book-cipher-algorithm/210603676

[18] Shumay, M., Srivastava, G., PixSel: Images as Book Cipher Keys // *Intl Journal of Electronics and Telecommunications*, 2018, Vol. 64, No. 2, pp. 151–158.

[19] Smart, N. *Cryptography: An Introduction (3rd Edition)*, New York, USA: McGraw Hill College, 2004, 433 p.

[20] Wang, C., Ju, S., A novel method to implement book cipher // *Journal Of Computers*, 2010, Vol. 5, No. 11, pp. 1621–1628.

[21] Wang, C., Ju, S., Book Cipher with Infinite Key Space // *2008 International Symposium on Information Science and Engineering*, Shangai, China: IEEE, 20-22 Dec., 2008, pp. 456-459. URL: https://ieeexplore.ieee.org/document/4732257.