Methods of information systems protection

UDC 519. 7 **doi:** https://doi.org/10.20998/2522-9052.2023.10

Farman Khubali Mammadov

Military Scientific-Research Institute of the National Defense University, Baku, Azerbaijan

NEW APPROACH TO BOOK CIPHER: WEB PAGES AS A CRYPTOGRAPHIC KEY

Abstract. Research relevance: Since ancient times, people have widely used methods of concealment and coding during information sharing, and ensuring the protection of information is currently relevant. Encryption methods are developing daily in order to ensure the reliable protection of confidential information and the exchange of data on the network. **The subject and purpose of the research** are to develop an encryption method, which is based on the ideology of book cipher and uses web pages as a cryptographic key, in the organization of a secure exchange of information. **The following tasks are solved in the article:** The article provides information about book cipher and analyzes modern methods of book cipher, as well as proposes a novel encryption method involving the use of web pages as a cryptographic key. **Research methods:** In the paper methods of analysis and synthesis are used. **Obtained results and conclusions:** The possibility of transforming the book cipher is proved, and a novel encryption method involving the use of web pages as a cryptographic key is proposed. The article also provides a comparison between the proposed encryption method involving the use of Internet pages as a cryptographic key with the classic book cipher method.

Keywords: cryptography; symmetric encryption; encryption algorithms; book cipher; cryptographic key; web pages as a key.

Introduction

In the decision-making process state bodies and officials, the significance of security and protection of information that contain a state secret increases. Because, in the condition of development of the information technologies, citizens are becoming subjects of information security due to their widespread use of banking operations, electronic commerce, online managed security systems, and so on. Malicious actions of ordinary people also contribute to the emergence of numerous security problems. On this basis, various protection methods have been developed, and new technologies, algorithms, and programs have been created to ensure information security. That’s why cryptographic solutions for solving these issues is critical in the organizations.

In order to ensure the protection of information during cryptographic encryption, the plaintext is transferred after being transformed into an incomprehensible form by the encryption algorithm and a key [1-3].

Regardless of how the information sharing is organized, the basic essence of the encrypted information must be changed in a way that, even if third parties gain access to it, only the receiving party may read or become familiar with the contents [4]. For this purpose, the cipher produced by cryptographic algorithms may consist of only letters, only numbers or mixed symbols.

The most important factors in ensuring reliable communication are considered to be the selection of the appropriate cryptographic algorithm and its most crucial parameter, which is the maximum 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 turns out that the issue of its delivery to the parties is the weakest point of the cryptosystem.

Various methods of delivering a key to parties have been developed in the literature. As an example, the numbered form of rows and columns of the Polybius square [5, p.173], binary codes for pictures [6; 7], a book [5, p.189; 8; 9], various files [10; 11] and a memorized poem [5, p.173] 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 [5, p.255; 12, p.665].

In addition to the fact that the encryption method, which uses books in academic, public, or commercial libraries as keys, has been used since ancient times, it has also been referred to in literature and cinematography. Despite the fact that the book cipher rule is considered one of the classical encryption methods, interest in it has always been great due to its widespread, simplicity of usage, as well as a large number of keys, and the difficulty of decryption in case of unknown key-book.

The research paper proposes an encryption method that is based on the ideology of book cipher and uses web pages as a cryptographic key. The article also gives information about book cipher and analyzes modern methods of book cipher, as well as provides a comparison between the encryption method, which involves the usage of web pages as a cryptographic key, and book cipher.

The book cipher

The use of book cipher became widespread with the invention of printing presses and the beginning of book printing. These events date back to the middle of the XIX century. The book cipher usage assumes that both parties involved in secret correspondence have the same book and copies of the same publication. In this case, it is required that the books are letter-for-letter identical [13].

The basic idea of a book cipher is that books are used as a cryptographic key, and the plaintext that needs to be encrypted is searched in the book word by word or letter by letter. Here, the word numbers, beginning with a certain letter, or the coordinates of the letters are the symbolic codes of the information being conveyed, in other words, the cipher. The cipher is often taken as the page number, paragraph number (sentence or line), word number, and letter number in the word. In this case, the letter used may correspond to several numbers or coordinates. The method is resistant to frequency attacks. Each letter in a secret code may correspond to several coordinates, the accuracy of which can only be established in the presence of an exact key. It means that the book used for encryption must be intercepted [13].

In one of the modifications of the Trisemus cipher, it is also proposed to use the book as a key. The parties (sender and recipient) agree to use a certain part of a particular book as a key. In this case, the length of the text fragment to be used as a key is taken equal to the length of the plaintext. Encryption is performed in the specified manner as in the Trisemus cipher. At the beginning of the ciphertext, a book page and a row number on this page are added to identify the encryption key [5, s.189].

Various revolutionary organizations in the Russian Empire widely used the book cipher throughout the late XIX - early XX century. The reason for this was the simplicity of mastering the method of methodical encryption and its resistance to attacks. Because the gendarmes' “black chambers”, which controlled confidential correspondence between members of organizations and were engaged in decrypting this data, had various methods of decryption, numerous opportunities, resources, supplies and reserves. Despite all this, the only disadvantage of the book cipher was logistics (book transportation). Because sometimes a book that was used as a key had to be kept or carried around covertly. When the suspect's possession of the same book was detected many times, it resulted in the disclosure and exposure of confidential correspondence [13]. There are no such limitations in the conditions of the daily development of the global Internet and the spread of web pages.

As a special case of a book cipher, there is also a method of poem encryption. A long poem that contains every letter of the alphabet is chosen or memorized in advance for the purpose of encryption. Each letter is replaced with two numbers during the encryption. The first of these numbers indicates the string in which this letter appears, while the second indicates the ordinal number in the string [5, s.189]. As an example, we can cite the correspondence between revolutionaries in Russia at the beginning of the XX century. N.A. Nekrasov's poem “Schoolboy” was used as a key in this correspondence. The text of the poem was written in a 10x10 square without any spaces and punctuation marks. If the number of letters in a string exceeded 10, the extra letters were removed [13].

Another approach to book cipher uses a dictionary. This guarantees the presence of almost all words and ensures verbatim encryption. In this case, each word of the plaintext is identified by the number of the page and the word on the page in the cipher. This method was used by George Scovell, Duke of Wellington, England, in some campaigns of the Peninsular War from 1807 to 1814. In the Scovell method, a number (dictionary page), a letter (letter on this dictionary page), and a number (word number) were used to encrypt each word in the cipher [14]. The extensive usage of dictionaries in this approach significantly reduces the robustness of the cipher. Because the combination of numbers-letters-numbers in the cipher allows professional cryptanalysts to easily determine whether the cipher was generated using any dictionary.

As a specific case of book cipher, there were cases of extensive use of the holy Bible book as a key. The numbers of chapters and verses make it simple to covertly convey any message and text in a method called the Biblical cipher [14].

During World War II, Richard Sorge skillfully used book cipher. Even after the Japanese captured Sorge, it was difficult for them to decipher the cipher of his spy ring in Japan until the correct key book was identified. Sorge for encryption had used a statistical handbook of Germany as a key [14]. In the American Revolution, General Benedict Arnold also applied a book cipher method and used William Blackstone's Commentaries on the Laws of England as a key [14].

The surveillance of persons conducting correspondence is the most effective method of attack aimed at decrypting cipher generated by the use of book cipher algorithms. In this case, special attention should be paid to the book and text that they are using to prepare secret information for a certain period of time. Rereading the same artwork repeatedly by one person might obviously arouse suspicions while surveillance. Especially when it is known that this person reads the same pages more often. Experts used to determine this by the dents on the pages. Obviously, carrying all the required books for encryption was a difficult task and might attract attention [13].

Modern approaches to book cipher

Although book cipher is related to classical methods, new approaches to it are being developed in the XXI century with the use of modern technologies. The following is an analysis of some modern ideologies developed on the basis of the book cipher method.

In [9], D. Ristanovic and J. Protic propose a new approach to the usage of the book cipher algorithm. The main idea of the proposed algorithm is to replace each symbol of the plaintext with the position of a certain letter of each word from the book taken as a key. During replacement, attention is paid to the fact that the location of the letters in the cipher is used only once.

While encrypting, the first and second letters of each word in the key book are taken, and a key file is created. Attention is paid to the fact that the key file contains all the letters of the alphabet, and the letters chosen are collected in a file in the sequence.

A system similar to the UUENCODE algorithm is used to encrypt symbols, numbers, and spaces in the plaintext that are not in the alphabet. The UUENCODE algorithm converts binary codes into text or vice versa, converts text into binary codes. During the usage of this system, it is assumed that all symbols, including spaces, will be converted to letters of the alphabet, and encryption will be performed this way.

The persons who will participate in the exchange of information must agree in advance on the key book and which letter of words will be used. When it is not determined in advance which letter of the words will be taken, the first letter of the words is taken into the key file.

When encrypting the next text by the agreed key book in the same session, one location is used once to increase the cipher's durability against crypto attacks. Therefore, after encrypting the first text, the location of the same letters in the key file is not used while encrypting the second text. The location of the last letter used when decrypting the first text is remembered, and the encryption of the second text is performed from this location. In this way, encryption of multiple plaintexts is possible. In case the encryption of plaintext is not completed and all locations in the key file are used up, then another key book must be taken to encrypt the plaintext.

During decryption, the pre-agreed letters of all the words in the agreed key book are sequentially collected into a key file. The plaintext is restored by extracting the letters from the key file according to the locations in the cipher.

The algorithm described above performs encryption with only one symbol or letter. Using the algorithm proposed in the article, it is possible to encrypt 4-5 symbols at once.

In [8], R.Lele, R.Jainani and others propose a modern encryption method based on a book. Although book cipher is related to classical cryptographic methods, the proposed approach considers and eliminates all the limitations. During encryption, the plaintext and an electronic book (in this case in PDF format), which will be used as a cryptographic key, are entered into the system. Then the relevant equivalent of each word that is present in the plaintext is searched in the key, and when it is found, the page number, row number, and word number of words of plaintext are taken as the cipher. When a word is not found in the key, it's divided into syllables, and a search is conducted for matching syllables. This rule applies to the word's letters if the search is unsuccessful. If the letter is not found, and there are numbers and symbols in the plaintext, encryption continues by the use of a database consisting of the alphabet and other symbols provided in the compiled program. Moreover, if there is more than one instance of a word in the plaintext and the key, and only one sample of a word is selected from the key, repetitions occur in the cipher, which, in turn, reduces the cryptographic strength of the algorithm against the frequency cryptanalysis method. To eliminate this disadvantage, a random function is used. This function randomly selects one of these samples to replace words in the plaintext by searching for several samples of the same word considered. As a result, a compression algorithm is used to reduce the volume of the generated ciphertext. The decryption operation is performed in reverse order.

In the encryption method proposed by R.Lele and others, only books and “pdf” files can be used as keys. However, in the method proposed in the article, it is possible to encrypt using a paragraph.

In [7], M.Shumay and G.Srivastava propose a new algorithm that is based on book cipher and uses images as a cryptographic key instead of a book. They call it the pixel counting method. The algorithm's main idea is based on using an image's pixels as a cryptographic key to encrypt any plaintext. Most “JPEG” or “PNG” images are encoded as pixels in computer systems using mainly 3 color channels (RED, GREEN and BLUE). And any pixel of the picture is a combination of the 3 8-bit values. In the proposed algorithm, encryption is performed using these color channels. First, the image to be used as a key is sectioned into blocks of 253 pixels from left-to-right and top-to-bottom. The most optimal block, which allows you to encrypt most of the symbols of the plaintext, is selected. The address of the optimal block is taken as a cipher. During encryption, the symbols of the plaintext are searched in a sequence of RED, GREEN and BLUE colors, and the indices of matching color codes are added to the cipher. That is, the first symbol is searched in RED, the second symbol is in GREEN, the third symbol is in BLUE, the fourth symbol is in RED again, and the search is continued in a similar manner and cipher is generated. If the symbols of the plaintext are not found in any block, then value 253 is placed as a marker in the cipher. Then, in the previous block, two pixels, the sum of which is equal to the relevant symbol, are searched and their indices are taken as a cipher. In order to perform encryption from the next color channel, value 254 is added to the cipher as a marker, and value 255 is added to define the end of encryption in the current block. In this way, encryption to the end of the plaintext is performed.

In the decryption proses, the address of block in the cipher’s first two bytes is read. Data from the key image is read until the markers according to the block and pixel numbers, read from the cipher, and the plaintext is restored. With a marker value of 253, the plaintext is restored by the sum of the information in the next two indices, with a value of 254, the plaintext is restored from the next color channel, and with a value of 255, the plaintext is restored from the indices of the next block.

The algorithm assumes the use of an image instead of a book, and the cipher consists of numbers. The method's main distinction is that encryption is performed at the bit level, not at the number level.

In [10] və [11], C.Wang və S.Ju, modifying the traditional book cipher, present a novel encryption method with infinite key space, which is immune from frequency cryptanalysis. The idea of the algorithm is based on the use of any file on the computer as a cryptographic key. The plaintext and the file taken as a cryptographic key are considered as binary codes. The plaintext is searched inside the key file, taking the form of bytes [11] or binary codes of arbitrary length [10].

The addresses of the identities found in the key are stored as keys. During decryption, the addresses in the cipher text are read from the key file and the plaintext is restored.

According to the ideology of the algorithm proposed by C.Wang və S.Ju, encryption is carried out at the level of binary codes, and files serve as the key. However, in the method proposed in the article, encryption is carried out at the symbol level, and files, as well as text fragments, can be used as a key.

New encryption method by using web pages as a cryptographic key

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 below shows the amount of information posted on some information sites in a day.

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 [15; 16; 17], the number of websites currently available on the Internet is over 1.4 billion. However, the number of active sites is only 17% of existing sites [16]. It is reported that the number of sites created daily around the world is more than half a million [15] or 250 thousand [16]. 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% [16].

Table 1 – **Amount of added information in some web sites**

Web site	Amount of 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

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-type information posted in social networks as cryptographic keys in the text encryption method proposed in the research paper.

The agreement process for the use of social network posts as a cryptographic key includes the web browser form of the social network platform, the web page and the publication on this page. To agree on a cryptographic key from text 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 networking 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 like 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 not recommended to use whole text of a web page 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.

As already mentioned, the main idea of the method is to perform position encryption using web pages as cryptographic keys. After the text that will be used as a cryptographic key is agreed between the parties, the plaintext (or mesasge) is divided into certain small pieces and searched for in the key. Plaintext fragmentation starts at the beginning of the text and is initially taken as four or five symbols. It is advisable to express the primary text in symbols rather than letters. Because when taking a text fragment, along with the letters of the words of the message, the fragment includes numbers, spaces, other punctuation marks and separators in the text. The initial number of symbols in the text can be increased or decreased at the user's request.

If a fragment of text is found in the text of the cryptographic key, then the initial value of the position in which the corresponding symbols of the key are located and the number of symbols in the text fragment are added to the cipher, and the next fragment of text is taken and searched in the key.

When the extracted plaintext fragment is not found in the cryptographic key text, the last character in the text fragment is discarded and the length of the fragment is reduced by one. A text fragment reduced by a length unit is searched in a key text. If there is a match, the initial value of the position where the matching key symbols are located and the number of symbols in the text fragment are added to the cipher. If the sequence of symbols in the text fragment is not found in the text of the cryptographic key, then the search is repeated, reducing the length of the text fragment by one. According to this rule, the length of the text fragment is reduced to one symbol.

Encryption is completed by dividing the plaintext into pieces or whole parts from the first letter to the last symbol. During encryption, the ciphertext is formed based on a value indicating the position of the plaintext fragment in the cryptographic key, and the number of symbols in the text fragment. That is, each piece of text is searched for by a key and its position in the key is determined. This position and the number of symbols in the text fragment is taken as the cipher. The resulting ciphertext consists mostly of numbers. The odd positions of the cipher contain the positions of the plaintext fragment in the cryptographic key, and the even positions contain the number of symbols in the fragment. At this point, no changes are being made to this web page or social media post. Then, to increase security, these numbers can be encrypted with one of the specific cryptographic algorithms, or hidden and sent to the other party by applying one of the existing steganographic methods.

To decrypt encrypted information, the receiving party first performs a primary decryption using the same methods of additional cryptographic and steganographic algorithms if they were used before. The cryptographic key is then taken from the agreed web page or social network page. According to the numbers in the odd position of the cipher, the position of the plaintext fragments is taken. The text is retrieved by taking the number of symbols in an even position in the cipher from the corresponding position in the cryptographic key.

Encryption and decryption operations are usually carried out as follows:

$$C = E_i(M); \quad (1)$$

$$M = D_k(C). \quad (2)$$

Here, *C* is a cipher, *M* is message, *E* and *D* are encryption and decryption algorithms, respectively and *k* – is a criptograhic key.

$$M = \overline{M_1, M_2, \ldots M_n}, \quad M_i \in A, i = 1..n; \quad (3)$$

$$K = \overline{K_1, K_2, \ldots K_s}, \quad K_j \in A, \ j = 1..s; \quad (4)$$

$$\begin{gathered} C = \overline{C_1, C_2, \ldots C_m}, \\ C_k \in \{1, 2, \ldots, 9999\}, \ k = 1..m. \end{gathered} \quad (5)$$

Here, *A* is an alphabet, *n* is a length of the plaintext, *i* is a plaintext's *i*-th symbol, *s* is a length of the cryptographic key, *j* is a cryptographic key's *j*-th symbol, *m* is a length of the cipher, *k* is a *k*-th number of the cipher.

Data (3)-(4) are set at the beginning of the encryption operation. The purpose of the encryption operation is to form a ciphertext (5) based on this data.

The expression for extracting a fragment of the plaintext, consisting of four symbols, during the encryption operation is shown in formula (6).

$$M_p = \overline{M_i, M_{i+1}, M_{i+2}, M_{i+3}}. \qquad (6)$$

Here M_p a piece of a text. In case $M_p \in K$ then numbers indicating the position of the cipher and the length of the text piece are added to the ciphertext.

Formula (7) depicts encrypted content:

$$C = \{P_1, R_1, P_2, R_2, \ldots, P_t, R_t\}. \qquad (7)$$

Here P is a starting number of the plaintext fragment that occurs in the key, R denotes the number of symbols in the fragment, t indicates the number of the last pair of message fragment in the cipher.

Total number of R in the cipher is equal to the length of the plaintext and is expressed as the following (8):

$$\sum_{i=1}^{t} R_t = n .$$

The number of P in cipher is less than or equal to the length of the plaintext. This is expressed as the following (9):

$$t \le n . \qquad (9)$$

Thus, the proposed method ensures the concealment of the fact of the presence of information when receiving and sending confidential information from one place to another using the listed options. 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.

Comparison of encryption by using a web page and a book

The proposed approach to using web pages as cryptographic keys incorporates some features of book encryption. However, the use of modern technologies distinguishes the new method from the existing ones.

As mentioned, there are some similarities and differences between the encryption method proposed in this paper using web pages, including web pages and social media posts as cryptographic keys, and book encryption. Similarly, both encryption methods use text type information as a cryptographic key to encrypt symbol combinations or single symbols. Another similarity is that the cryptographic key involved in the encryption process is used in a way available to everyone. The differences between the method proposed in the paper and book encryption can be considered as follows:

– Book encryption algorithms use books as cryptographic keys. However, in the proposed algorithm, web pages and social network posts are used as keys;

– Book encryption algorithms use the text of the book as a cryptographic key. That is, the question of using some part of it as a cryptographic key is not considered. However, in the proposed method, any fragment of a web page or extracted text, as well as a combination of fragments, can be used as a cryptographic key;

– In book encryption algorithms, word or symbol encryption must be agreed in advance. In the proposed algorithm, the length of the text fragment is determined on the encryption side. There is no need to inform the other party. During decoding, the original text is restored by deleting symbols from the corresponding position in the length of the text fragment specified during encryption;

– In the book cipher method, the cipher consists of a page, paragraph, line, word, or letter number. There are five parameters involved, three of which must be valid. However, the encryption of the proposed algorithm consists of only two parameters. To encrypt each symbol of the plaintext in the sequential replacement of characters in the book encryption method, at least three parameters and a separator between them are used. If the replacement occurs within the first 9 pages of the book, the first 9 lines of the page, and the first 9 words of the line, then at least 6 symbols for each character are added to the cipher, otherwise 9 symbols. If the encryption uses five book parameters instead of three parameters, then encryption is performed using 8 or 11 characters for each symbol, respectively. In the proposed method, encryption is performed using two parameters in encryption. In this case, the length of the cryptographic key plays an important role. So, if the key length consists of decimal numbers, 5 symbols are added to the ciphertext for each operation, and if the length is hundredths, then 7 symbols are added for each operation;

– When encrypting a book, there is no approach to encrypt the missing characters of the plaintext in the book, but the proposed method provides a solution to the problem of encrypting the missing symbols.

Conclusions

In the modern world, in the conditions of widespread and accessible information technologies, the possibility of transforming the book cipher has been proved, taking into account the fact that data is stored in the form of files on computers. The article proposes a new encryption method by using web pages as cryptographic keys on the basis of the book encryption ideology. The article provides information about encryption using the book, an analysis of modern encryption methods using the book, as well as a comparison of the encryption method using Internet pages as a cryptographic key. Moreover, a method has

been developed for identifying and consenting to the use of web pages and social media posts as cryptographic keys. It is shown that the proposed method allows to encrypt and decrypt web pages, as well as pages of social networks using cryptographic keys. There is a prospect to do some work in the future in the field of developing new encryption methods using the proposed method.

REFERENCES

1. Barker, E.B., Roginsky, A.L. & Davis, R. (2020), *Recommendation for Cryptographic Key Generation*, National Institute of Standards and Technology (NIST), Gaithersburg, USA, Special Publication (SP) 800-133, Rev. 2., 36 p., doi: https://doi.org/10.6028/NIST.SP.800-133r2
2. Elizabeth, D. & Denning, R. (1982), *Cryptography and data security*, Addison-Wesley Publishing Company, USA and Canada, Inc., 404 p.
3. Ferguson, N. Schneier, B. & Kohno, T. (2010), *Cryptography Engineering: Design Principles and Practical Applications*, Wiley Publishing, Indianapolis, Indiana, USA: 353 p.
4. Churchhouse, R.F. (2004), *Codes and Ciphers. Julius Caesar, the Enigma and the internet*, Cambridge University Press, Cambridge, UK, 240 p.
5. Gasimov, V.A. (2009), *Informasiya tehlukesizliyinin esaslari* [*Fundamentals of information security. Textbook*], MNS MTS Main Department Publishing Center, Baku, Azerbaijan, 340 p. (in Azerbaijani)
6. Alqad, Z., Oraiqat, M., Almujafet, H., Al-Saleh, S., Husban, H.Al & Al-Rimawi S. (2019), "A New Approach for Data Cryptography", *International Journal of Computer Science and Mobile Computing*, Vol. 8, Is. 9, pp. 30-48.
7. Shumay, M. & Srivastava, G. (2018), "PixSel: Images as Book Cipher Keys", *Intl Journal of Electronics and Telecommunications*, Vol. 64, No. 2, pp. 151–158. doi: https://doi.org/10.24425/119363
8. Lele, R. Jainani, R., Mikhelkar, V. & Nade A. (2014), "The Book Cipher Optimised Method To Implement Encryption And Decryption", *International journal of scientific & technology research*, Volume 3, Issue 1, pp. 11-14.
9. Ristanovic, D. & Protic, J. (2008), "The Book Cipher Algorithm", *Dr. Dobb's Journal*, October, pp. 48-51, URL: drdobbs.com/security/the-book-cipher-algorithm/210603676
10. Wang, C. & Ju, S. (2010), "A novel method to implement book cipher", *Journal Of Computers*, Vol. 5, No. 11, pp. 1621–1628, doi: http://dx.doi.org/10.4304/jcp.5.11.1621–1628
11. Wang, C. & Ju, S. (2008), "Book Cipher with Infinite Key Space", *2008 International Symposium on Information Science and Engineering*, Shangai, China: IEEE, pp. 456-459, doi: http://dx.doi.org/10.1109/ISISE.2008.273
12. Aliguliyev, R.M. & Imamverdiyev, Y.N. (2006), *Kriptoqrafiyanın əsasları* [*Fundamentals of Cryptograpy*], Baku, Azerbaijan: Publishing House "Information technologies", 688 p. (in Azerbaijani)
13. Dushkin R.B. & Yaxontov, S.I. (2021), "Knijniy shifr [Book Cipher]", *Potential. Mathematics. Physics. Informatics*, No. 03, pp. 45–49. (in Russian)
14. (2022) *Book Cipher*, URL: https://cryptography.fandom.com/wiki/Book_cipher (16.03.2022).
15. (2022) *How Many Websites Are There?* URL: https://websitesetup.org/news/ how-many-websites-are-there/ (28.11.2022).
16. Huss, N. (2022), *How Many Websites Are There in the World?* URL: https://siteefy.com/how-many-websites-are-there/ (03.12.2022).
17. (2022) *Total number of Websites*, URL: https://www.internetlivestats.com/total-number-of-websites/ (15.12.2022).

Received (Надійшла) 12.12.2022
Accepted for publication (Прийнята до друку) 08.02.2023

ВІДОМОСТІ ПРО АВТОРІВ / ABOUT THE AUTHORS

Мамедов Фарман Хубалі – аспірант, Військовий науково-дослідний інститут Національного університету оборони, Баку, Азербайджан;

Farman Khubali Mammadov – postgraduate student of the Military Scientific-Research Institute of the National Defense University, Baku, Azerbaijan;

e-mail: fermanmemmedov@gmail.com; ORCID ID: http://orcid.org/0000-0002-0604-6996.

Новий підхід до книжкового шифру: веб-сторінки як криптографічний ключ

Ф. Х. Мамедов

Анотація. Актуальність дослідження: З давніх часів люди широко використовували методи приховування та кодування під час обміну інформацією, і забезпечення захисту інформації є актуальним в даний час. Методи шифрування щодня розвиваються, щоб забезпечити надійний захист конфіденційної інформації та обмін даними в мережі. **Предметом і метою дослідження** є розробка методу шифрування, який базується на ідеології книжкового шифру та використовує веб-сторінки як криптографічний ключ, для організації безпечного обміну інформацією. У статті вирішуються наступні завдання: у статті наводиться інформація про книжковий шифр та аналізуються сучасні методи книжкового шифрування, а також пропонується новий метод шифрування з використанням веб-сторінок як криптографічного ключа. **Методи дослідження:** У роботі використовуються методи аналізу та синтезу. **Отримані результати та висновки:** доведено можливість трансформації книжкового шифру та запропоновано новий метод шифрування з використанням веб-сторінок як криптографічного ключа. У статті також проведено порівняння запропонованого методу шифрування з використанням інтернет-сторінок як криптографічного ключа з класичним методом книжкового шифру.

Ключові слова: криптографія; симетричне шифрування; алгоритми шифрування; книжковий шифр; криптографічний ключ; веб-сторінки як ключ.