AiMT

Advances in Military Technology
Vol. 14, No. 1 **(2019)**, pp. 79-88
ISSN 1802-2308, eISSN 2533-4123
DOI 10.3849/aimt.01281

From Old Ciphers to Modern Communications

C. Flaut[1], D. Flaut[2], S. Hoskova-Mayerova[3*] and R. Vasile[1]

[1] *Faculty of Mathematics and Computer Science, Ovidius University of Constanța, Rumania*
[2] *Faculty of History and Political Sciences, Ovidius University of Constanța, Rumania*
[3] *Department of Mathematics and Physics, University of Defence, Brno, Czech Republic*

The manuscript was received on 30 November 2018 and was accepted
after revision for publication 15 March 2019.

Abstract:

The security of the information transmitted, irrespective of the era and the channel selected, has always been one of the main concerns of those using various communication systems. This is particularly the case nowadays, when the Internet has made the mass distribution of any kind of information possible. Codes can be used to transmit data through various noisy channels and any errors that might occur can be corrected; it is therefore very important to design gappropriate codes with adequate parameters. This survey briefly outlines the evolution of the ways in which information has been collected, transmitted and used from the past to the present.

Keywords:

code, crypto–system, communication

1 Introduction

In the text that follows, we intend to cast a backward glance and draw a brief comparison between the ways in which information was collected, transmitted and used in the past and those employed in the present.

Information security has gone through a variety of stages, from the simple process of encrypting and decrypting information and delivering it through an emissary, which can be regarded as the first channel of communication, to the elaborate attempts to persuade the person holding the information to reveal it. Even though some information may hold no actual value to its custodian, it can easily gain considerable importance if it falls in the hands of people that can use it to their advantage, for personal gain. It is generally quite easy to get hold of someone's personal data, without the person in question experiencing any sense of loss. However, the collected personal data of several people can be of value to a marketing agency, for instance see [1].

An entire field, known as social engineering, has thus emerged. This field concerns itself with obtaining information or gaining access to various secured systems, manipulating those

* *Corresponding author: Department of Mathematics and Physics, Faculty of Military Technology, University of Defence, Kounicova 65, 662 10, Brno, Czech Republic. Phone: +420 973 44 22 25, E-mail: sarka.mayerova@unob.cz.*

who own them or have legitimate access to them by means of various fraudulent or legal strategies. The main aim pursued in this field entails gaining the confidence of the chosen targets in order to make them disclose important information or to grant access to the secured system that needs to be breached. Such strategies rely on various psychological factors (naivety, vanity, irresponsibility, greed), as well as on a range of ways of drawing attention away from important issues or taking advantage of human automatisms. This is why social engineering strategies are employed with increasing frequency in the fiercely competitive present-day market [2]. The aspects outlined below, to do with collecting and using apparently trivial information, are only new in terms of the strategies involved and the levels where they are applied. In fact, the ideas on which such actions are based are extremely old, it is only the shape they take and the modus operandi that are new.

In the text that follows, we intend to cast a backward glance and draw a brief comparison between the ways in which information was collected, transmitted and used in the past and those employed in the present.

2 Some Historical Aspects

In the past, information was sometimes transmitted by means of people functioning as communication channels, delivering usually encrypted messages to their destination. In addition, they were also in charge of collecting information which, in turn, was transmitted back to the people employing them. For instance, they would stop at an inn and strike up a conversation with the innkeeper or patrons, thus becoming aware of a wide range of issues.

Various types of ciphers were used to encode the messages transmitted. For a long period of time, use was made of the so-called classical ciphers or mono-alphabetic ciphers, comprising two varieties: transposition and substitution.

Transposition entailed a mere rearrangement of the letters, which was quite difficult to use, especially when the messages were decoded. The Spartan scytale was the earliest such means of rearranging letters. It consisted of a piece of wood of a certain length and thickness, which represented in fact the encoding and decoding key, with a strip of leather wound around it on which the message was written. The unwound strip of leather contained the mixed-up message. The recipient had an identical scytale, around which he could wind the strip of leather in order to read the text to be transmitted [3, p. 12].

Substitution represented another variety of mono-alphabetic cipher in which every letter was replaced with another one, according to a pre-established rule, which represented in fact both the encrypting and the decrypting key. One such cipher was Caesar's Cipher, in which each letter was replaced with a letter three positions down the alphabet [4, p. 48–69]. A problem posed by these ciphers was that they were easy to break by means of certain statistical data to do with the text transmitted, that is by applying a so-called frequency analysis to the letters in the text. After the discovery of this method, credited to the Arab mathematician Al-Kindi in the 9^{th} century, many of the encryption methods previously used became vulnerable, the ciphers being easy to crack, see [5], [3, p. 22]. This became more of a challenge when poly-alphabetic ciphers appeared, presumably introduced by Leon Battista Alberti around 1467. These new codes used distinct mono-alphabetic ciphers for different parts of the message transmitted. A simple variety of poly-alphabetic substitution is the Vigenère cipher, which seems to have been known long before its first appearance in print. In 1586, Blaise de Vigenère published A Treatise on Secret Writing in which he described this cipher [6, p. 35–37].

A famous instance in which the use of a specific cipher played an important part was

the case of Mary, Queen of Scots, who was involved in an assassination plot targeting Queen Elizabeth I. The letters in which she outlined this plot were encrypted by means of an ostensibly unbreakable cipher, an improvement on the mono-alphabetic cipher with symbols arranged in a nomenclator. This cipher eventually turned out to be easy to crack, and Mary Stuart was brought to trial and sentenced to death by beheading on 8 February 1587 [7].

The idea of adding the key to the text, the technique entailed by the Vigenère cipher, had been known for a long time, but it would appear that Vigenère was the first to make it public. At the time, few institutions allowed the study of encrypted texts, monasteries being among them [3, p. 31]. This is the reason why there are many known instances in which this encoding method was employed not only in diplomacy but also in certain church books, such as the London Gospel transcribed by Radu of Măniceşti in 1574. This encoding method was also used in the case of certain encrypted inscriptions found on the walls of Humor Monastery in the north of Moldavia, Romania [8]. In this encoded text, the Cyrillic letter H corresponded to the letter group DD. Indeed, if we label the letters of the Cyrillic alphabet, the letter D corresponds to 4, and H to 8. Therefore, the letter H can be encoded as the sum of letter labels D and D, that is $DD = 4 + 4 = 8 = H$ [5], [9, p. 376–378].

In brief, the Vigenère cipher used as its key a word of certain length associated with a number obtained from the labels attached to the letters making up the key. In actual fact, the Vigenère cipher is a series of texts encoded by means of the Caesar Cipher and different keys provided by the letter labels of the key word. If one knows the length of the key used to encode the text, the latter can be decoded. It can be noted that if we were to know the length L of the key, the rest would be a matter of analysing L texts encoded with Caesar ciphers entailing different keys.

The Vigenère cipher was considered unbreakable for a long time. It was eventually cracked by Charles Babbage in 1854 as well as by Friedrich Kasiski in 1863. The technique used for this purpose was put forward by both Babbage and Kasiski, independently of one another, but for unknown reasons Babbage never published it, see e.g. [3, p. 73], [10]; [11, p. 196].

In 1837 Charles Babbage became the first person to design a programmable calculating machine, the Analytical Engine, which can be regarded as a precursor of modern computers. However, due to the technical limitations of the period, this machine could not be built at the time. In 1843 Ada Lovelace wrote an algorithm that could be processed by this machine, making history as the world's first programmer [12].

As mentioned above, finding out the length of the key used to encrypt a text by means of the Vigenère cipher allows the text to be decrypted. One of the methods employed to discover the length of the key is the Kasiski examination, which he came up with in 1863. In order to determine the length of the key, one needs to count the occurrences of the letters that match when the encrypted text is compared against the actual text, displaced by a certain number of positions, which can provide the possible length of the key. The distance must be determined for every such pair. The value of length L of the key is going to be the greatest common divisor or a divisor of the latter. After establishing the length of the key, letter frequency analysis is conducted on a text in the L subtexts, $S_1, S_2, \ldots, S_L$ determined as follows: S_1 consists of the letters from the encrypted text located at $1, L + 1, 2L + 1$, etc. S_2 consists of the letters from the encrypted text located at $2, L + 2, 2L + 2, \ldots$ and so on [13, p. 45–100], [14, p. 36].

Another way of finding out the length of the encryption key, established by Wolfe Friedman in 1920, employs the index of coincidence I. If we have a sequence of m characters, the probability of finding out that two arbitrarily selected characters are identical is known as

index of coincidence. If letters $A, B, C, \ldots, Z$ appear in the length m de m_0, m_1,..., m_{25} times respectively, so that

$$m = m_0 + m_1 + ... + m_{25}, \tag{1}$$

then the index of coincidence is

$$I = \frac{m_0 (m_0 - 1) + m_1 (m_1 - 1) + ... + m_{25} (m_{25} - 1)}{m (m - 1)}, \tag{2}$$

and the key length is probabilistically determined and is approximately

$$L \approx \frac{0.027m}{(0.065 - I) + m(I - 0.0385)}. \tag{3}$$

More details can be found in [15], [14, p. 36].

The appearance of the electrical telegraph built by Alfred Vail and Samuel Morse in 1844, as well as the first radio transmission conducted in 1894 by Guglielmo Marconi, who employed his own equipment, made it possible to deliver information by means of these new methods much faster and more efficiently than by sending an emissary [16, 17].

In an endeavour to make it easier to encrypt and decrypt secret messages, the German inventor Arthur Scherbius built an electromagnetic machine initially used for commercial purposes, named the Enigma machine. During World War Two, the Enigma was consistently used to encrypt messages. The machine had a keyboard, a lamp panel and a set of rotors. The keyboard was used to enter the plain, non-encrypted text, which resulted in encrypted symbols at the level of the lamp panel, via the rotors. The movement of the rotors was meant to apply a different key when the keyboard was touched [3, p. 105].

One of the mathematicians to point out the shortcomings of the Enigma machine during World War Two was Alan Turing. He joined the code breakers of Bletchley Park, an estate from the town of Bletchley and the headquarters of the cryptanalysts that succeeded in cracking the Enigma machine codes. Alan Turing created the Turing machine, which can be considered one of the ancestors of present-day computers [18].

The appearance of the Internet in 1969 revolutionised means of communication. The Internet (short for interconnected networks) is a global network developed by connecting several computer networks from around the world by means of specific communication rules known as Protocols. The Internet started as an experimental project run by an agency within the United States Department of Defense. This project, initially called ARPANet, connected computers from the University of California, Los Angeles to those belonging to the Stanford Research Institute [19]. The ARPANet project also played a major role in the emergence of the email service. In 1971, Ray Tomlinson, a Geneva physicist, set up an electronic mail (email) system based on the ARPANet network, choosing the @ symbol to send messages from one computer to another [20].

Over the last few years, wireless networks have evolved considerably worldwide. The technology used in the case of wireless communication can connect various pieces of equipment notwithstanding the distance between them. The widespread use of these networks led to the development of new technologies which can provide their users with quality services, such as extremely fast communication, as well as safety through new ways of increasing transmission security.

3 Some Mathematical Aspects

As seen above, these means of communication, whether new or old, are based on various mathematical notions: encrypting and decrypting algorithms, mathematical items employed in the construction of advanced codes used to transmit information, etc. It can therefore be argued that Mathematics played an important part in the development of these fields.

3.1 The RSA-Cryptosystem

Invented in 1978 by Ron Rivest, Adi Shamir and Leonard Adleman, RSA is one of the best known public key cryptosystems and it is based on the difficulty of factoring big numbers.

Choosing two very large prime numbers, with more than 100 digits each, we consider $n = pq$. Computing Euler's totient function for the natural number n, we obtain

$$\varphi(n) = (p-1)(q-1). \tag{4}$$

We randomly choose an integer e between 1 and $\varphi(n)$ such that e and $\varphi(n)$ are coprime. We consider $\{n, e\}$ the public key. Since $\gcd[e, \varphi(n)] = 1$, we can find the inverse modulo $\varphi(n)$, denoted by d. It is clear that $ed = 1 \bmod \varphi(n)$. The number d will be the secret key. Supposing that the plain text is $m, m < n$, we have the encryption function

$$c = m^e \bmod n. \tag{5}$$

The decryption function is

$$m = c^d \bmod n. \tag{6}$$

For more details see [21, p. 83–96].

It is clear that if we know the exponent e, finding the decryption key d is equivalent to the factorization of the number n. For n as a large integer, such a thing is practically impossible. Since there are factorizing tests, such as for example "rho"–test, Pollard's $p-1$ method, the Lenstra elliptic-curve factorization method or the Number Field Sieve test, which can factorize large numbers, some precautions are necessary when choosing the numbers p, q and e. We have to note that the prime numbers p and q must be chosen in such a way that $p-1$ and $q-1$ have a large prime factor and are not too close to one another. The integer e must be chosen in such a way so as not to be too small and n must have a minimum of 1024-bits [14, p. 43–50, p. 52–53], [22].

3.2 DES and AES Cryptosystems

DES (Data Encryption Standard) is a symmetric cryptosystem used from 1976 until 2001 as the international encryption standard. Since DES was considered unsafe due to the short length of the key, in 2001 it was replaced with AES (Advanced Encryption Standard), a block cipher which uses $\mathbb{Z}_2$ as its alphabet. Starting from this year, AES is intensively used around the world as the encryption standard [23, p. 127–136, p. 139–148].

4 Codes

Codes can be used to transmit data through various noisy channels and any errors that might occur can be corrected; it is therefore very important to design good codes with adequate parameters. Some examples of such codes are provided below.

The Hamming codes can detect two errors and correct one error. These codes are used when errors are rare, as is the case for example with the computer memory system (RAM) [24].

The Golay codes were discovered by M. J. E. Golay in 1949. These codes are linear error correcting codes used in digital communications. For example, these codes were used in 1977 for encoding and decoding the data for the Voyager space missions [25], [26, p. 88].

The Reed–Muller codes discovered in 1954 by D.E. Muller are error-correcting codes used particularly in space communications. They were used by the NASA space probe Mariner 9 to transmit black and white pictures from Mars to Earth in 1972 [26, p. 118], [27].

4.1 Space Time Block Codes

Quaternions were discovered in 1843 by Sir William Rowan Hamilton and have many applications, one of which is in Coding Theory [28]. We consider the real quaternion algebra $\mathbb{H}$ with basis $\{1, i, j, k\}$, where

$$i^2 = j^2 = k^2 = -1, ij = -ji, ik = -ki, jk = -kj, \tag{7}$$

each element in $\mathbb{H}$ takes the form $q = a + bi + cj + dk, a, b, c, d \in \mathbb{R}$.

If we consider an arbitrary field K, with $charK \neq 2$, and the elements $\alpha, \beta \in K$, the generalized quaternion algebra $\mathbb{H}(\alpha, \beta) = \left(\frac{\alpha,\beta}{K}\right)$ is a four dimensional algebra with basis $\{1, f_1, f_2, f_3\}$, and the multiplication given in the following Tab. 1.

Tab. 1. Multiplication table

$\cdot$	1	f_1	f_2	f_3
1	1	f_1	f_2	f_3
f_1	f_1	α	f_3	αf_2
f_2	f_2	$-f_3$	β	$-\beta f_1$
f_3	f_3	$-\alpha f_2$	βf_1	$-\alpha\beta$

If $a \in \mathbb{H}(\alpha, \beta)$, $a = a_0 + a_1 f_1 + a_2 f_2 + a_3 f_3$, we define

$$\mathbf{t}(a) = a + \overline{a} \in K, \tag{8}$$

and

$$\mathbf{n}(a) = a\overline{a} = a_0^2 - \alpha a_1^2 - \beta a_2^2 + \alpha\beta a_3^2 \in K, \tag{9}$$

called the trace and the norm of the element $a \in \mathbb{H}(\alpha, \beta)$.

If for $x \in \mathbb{H}(\alpha, \beta)$, the relation $\mathbf{n}(x) = 0$ implies $x = 0$, therefore the algebra $\mathbb{H}(\alpha, \beta)$ is called a *division algebra*. Otherwise, it is called a *split algebra*. We observe that the algebra $\mathbb{H}(-1, -1) = \left(\frac{-1,-1}{\mathbb{R}}\right)$ is a division algebra. For details regarding quaternions, readers are referred to [29].

A block code is an error-correcting code which encodes data in blocks. Space-Time Block Codes are used in wireless communications systems with multiple antennas, ensuring the high reliability of the transmission. Due to their properties, complex numbers and division quaternion algebras were used to build Space Time Block Codes. The Alamouti code, designed in 1998, is one such example [30]. The code is given by the following set

$$\mathcal{C}=\left\{\left(\begin{array}{cc} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{array}\right) \mid z_1, z_2 \in \mathbb{C}\right\}, \tag{10}$$

where z_1, z_2 are two complex numbers which represent information symbols.

For $Z, Y \in \mathcal{C}$, we note that

$$\det(Z-Y)=|z_1-y_1|^2+|z_2-y_2|^2 \geq 0. \tag{11}$$

This property is called *full diversity*. From the operations above, it follows that code $\mathcal{C}$ can be given as the left representation of $\mathbb{H}$ over $\mathbb{C}$

$$\lambda: \mathbb{H} \rightarrow M_2(\mathbb{C}), \lambda(q)=\left(\begin{array}{cc} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{array}\right), \tag{12}$$

where $q=z_1+z_2 j$. For $Z=\left(\begin{array}{cc} z_1 & -\overline{z_2} \\ z_2 & \overline{z_1} \end{array}\right)$, we have $\det Z=\mathbf{n}(q)$ and $\mathbf{n}(q)=0$ implies $q=0$. Therefore, the full diversity property is equivalent to the division property of the algebra $\mathbb{H}$, see [31, 32, 33].

5 Codes and BCK–algebras

Certain algebraic structures have lately been associated to various types of codes. A question to ask in this respect is: Who influences whom? Is it the case that the properties of algebraic structures can lead to the elaboration of good codes, or that the attached codes can lead to the discovery of new and interesting properties of these algebraic structures?

Let X be a nonempty set, "$*$" be a binary relation defined on X and $\theta \in X$ be a constant element. The pair $(X, *, \theta)$ is called a set of $(2,0)$ type.

A set $(X, *, \theta)$ of $(2,0)$ type is called a *BCI algebra* if the following condition are satisfied:

1) $((x*y)*(x*z))*(z*y)=\theta$, for all $x, y, z \in X$;

2) $(x*(x*y))*y=\theta$, for all $x, y \in X$;

3) $x*x=\theta$, for each $x \in X$;

4) For each $x, y, z \in X$ such that $x*y=\theta, y*x=\theta$, we obtain $x=y$.

If a BCI algebra X satisfies the following relation:

5) $\theta*x=\theta$, for each $x \in X$, therefore X is called a *BCK algebra.* These algebras were introduced for the first time in 1966 by Y. Imai and K. Iseki in [34].

One of the recent applications of BCK-algebras was given in the Coding Theory. In the paper [35], the authors constructed a finite binary block-code associated to a finite BCK-algebra. At the end of the paper, they raised the question of whether the converse of this statement was also true. In [36] an answer was given to this question: under some circumstances, the converse is also true. Therefore we can associate a finite BCK algebra to a finite binary block code. The algorithm developed here can be extended to other algebraic structures.

6 Conclusions

The security of the information transmitted, irrespective of the era and the channel selected, has always been one of the main concerns of those using various communication systems. This is particularly the case nowadays, when the Internet has made the mass distribution of any kind

of information possible. Mathematics has played an important part in this endeavour through the various algorithms elaborated to enable communication, via both old and modern means.

Acknowledgements

The work presented in this paper was supported within the project for Development of basic and applied research developed in the long term by the departments of theoretical and applied bases FMT (Project code: DZRO K-217) supported by the Ministry of Defence of the Czech Republic.

References

[1] CIALDINI, R. B. *Influence: The Psychology of Persuasion*. HarperCollins, 1984, 334 p. ISBN 978-0-061-24189-5.

[2] *Social Engineering Defined* [on-line]. [cited 2018-11-05]. Available from: https://www.social-engineer.org/framework/general-discussion/social-engineering-defined.

[3] SINGH, S. *The Code Book-How to Make it, Break it, Hack it, Crack it*. Delacorte Press, 2001, 263 p. ISBN 978-0-385-72913-0.

[4] MARTIN, K. *Everyday Cryptography*. Oxford: Oxford University Press, 2012, 720 p. ISBN 978-0-198-78801-0.

[5] FLAUT, C. and FLAUT, D. Cryptographic Systems Used in the Romanian Countries between the 15^{th} – 19^{th} Centuries. *Asian Journal of Social Sciences & Humanities*, 2015, vol. 4, no. 1, p. 109–117. ISSN 2186-8492.

[6] WOBST, R. *Cryptology Unlocked*. Wiley, 2001. 557 p. ISBN 978-0-470-06064-3.

[7] *Encyclopaedia Britannica Online-2* [on-line]. [cited 2018-11-04]. Available from: https://www.britannica.com/place/ United-Kingdom/Elizabethan-society#ref483014.

[8] BALŞ, Ş. *The Humor Monastery*. Bucharest: Meridiane Publishing House, 1965, 30 p.

[9] MAREŞ, A. *Old English Writing and Culture* [in Rumanian]. Bucarest: Academiei Române, 2005, 486 p. ISBN 978-3-598-20437-1.

[10] *Encyclopaedia Britannica Online-3* [on-line]. [cited 2018-10-05]. Available from: https://www.britannica.com/topic/ cryptology/Cryptography#ref392519.

[11] KLIMA, R. E. and SIGMON, N. P. *Cryptology: Classical and Modern with Maplets*. Boca Raton: CRC Press, 2012.

[12] *Encyclopaedia Britannica Online-1* [on-line]. [cited 2018-10-14]. Available from: https://www.britannica.com/ biography/Charles-Babbage.

[13] SINGH, S. *The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography*. London: Fourth Estate, 1999.

[14] SCHAEFER, E. *An Introduction to Cryptography* [on-line]. Santa Clara: Santa Clara University, 2005, [cited 2018-10-14]. Available from: http://cgi.di.uoa.gr/~halatsis/Crypto/Bibliografia/Crypto_Lectures/ Schaefer_intro_crypto.pdf.

[15] CHRISTENSEN, C. *Cryptanalysis of the Vigenère Cipher: The Friedman Test* [on-line]. MAT/CSC 483, 2015. [cited 2018-10-14]. Available from: https://www.nku.edu/~christensen/ 1402%20Friedman%20test%202.pdf.

[16] *Encyclopaedia Britannica Online-4* [on-line]. [cited 2018-11-05]. Available from: https://www.britannica.com/ biography/Samuel-F-B-Morse.

[17] *Encyclopaedia Britannica Online-5* [on-line]. [cited 2018-11-05]. Available from: https://www.britannica.com/ biography/Guglielmo-Marconi.

[18] *Encyclopaedia Britannica Online-6* [on-line]. [cited 2018-11-05]. Available from: https://www.britannica.com/ biography/Alan-Turing.

[19] GROMOV, G. *Roads and Crossroads of Internet History* [on-line], 1995, [cited 2018-11-05]. Available from: http://history-of-internet.com/history_of_internet.pdf.

[20] GRAHAM, F. *Clash of the Titans: Email v Social Media* [on-line], 2011, [cited 2018-11-05]. Available from: https://www.bbc.com/news/business-15856116.

[21] KOBLITZ, N. *A Course in Number Theory and Cryptography*. Springer-Verlag, 2nd edition, 1994, 235 p. ISBN 978-0-387-94293-3.

[22] CASE, M. *A Beginner's Guide To The General Number Field Sieve*. Corvallis: Oregon State University, ECE 575, 2003, 19 p.

[23] BUCHMANN, J. *Introduction to Cryptography*. Springer-Verlag, 2nd edition, 2004, 338 p. DOI 10.1007/978-1-4419-9003-7.

[24] MALEK, M. *Coding Theory-Binary Hamming Codes* [on-line], 2015, [cited 2018-11-05]. Available from: http://www.mcs.csueastbay.edu/~malek/Class/Hamming.pdf.

[25] MALEK, M. *Coding Theory-Golay Codes* [on-line], 2015, [cited 2018-11-05]. Available from: http://www.mcs.csueastbay.edu/~malek/Class/Golay.pdf.

[26] LING, S. and XING, C. *Coding Theory A First Course*. Cambridge:Cambridge University Press, 2004, 222 p. ISBN 978-0-521-82491-9.

[27] MULLER, D. E. Application of Boolean Algebra to Switching Circuit Design and to Error Detection. *Transactions of the I.R.E. Professional Group on Electronic Computers*, 1954, vol. 3, p. 6–12. DOI 10.1109/IREPGELC.1954.6499441.

[28] BAEZ, J. C. The Octonions. *Bulletin of the American Mathematical Society New Series*, 2002, vol. 39, no. 2, p. 145–205.

[29] SCHAFER, R. D. *An Introduction to Nonassociative Algebras*. New-York: Academic Press, 1966, 165 p. ISBN 978-04-86688138.

[30] ALAMOUTI, S. M. A Simple Transmit Diversity Technique for Wireless Communications. *IEEE Journal on Selected Areas in Communications*, 1998, vol. 16, no. 8, p. 1451–1458. ISSN 0733-8716, DOI 10.1109/49.730453.

[31] PUMPLŰN, S. *How to Obtain Division Algebras Used for Fast Decodable Space-Time Blocks Codes*, *Advances in Mathematics of Communications*, 2014, 8 (3) : 323-342. DOI 10.3934/amc.2014.8.323, [on-line], 2013, [cited 2018-11-05]. Available from: http://molle.fernuni-hagen.de/~loos/jordan/archive/iteralg/iteralg.pdf.

[32] PUMPLŰN, S. and UNGER, T. Space-time Block Codes from Nonassociative Division Algebras. *Advances in Mathematics of Communications*, 2011, vol. 5 no. 3, p. 449–471. DOI 10.3934/amc.2011.5.449.

[33] UNGER, T. and MARKIN, N. Quadratic Forms and Space-Time Block Codes from Generalized Quaternion and Biquaternion Algebras. *IEEE Transactions on Information Theory*, 2011, vol. 57, no. 9, p. 6148–6156. ISSN 0018-9448, DOI 10.1109/TIT.2011.2161909.

[34] IMAI, Y. and ISEKI, K. On Axiom Systems of Propositional Calculi. *Proceedings of the Japan Academy*, 1966, vol. 42, p. 19–22. DOI 10.3792/pja/1195522169.

[35] JUN, Y.B. and Song, S.Z. Codes Based on BCK-algebras. *Information Sciences*, 2011, vol. 181, no. 22, p. 5102–5109. DOI 10.1016/j.ins.2011.07.006.

[36] FLAUT, C. BCK-algebras Arising from Block-codes. *Journal of Intelligent & Fuzzy Systems*, 2015, vol. 28, p. 1829–1833. DOI 10.3233/IFS-141469.