Algorithmic Support for Rabin Cryptosystem Implementation Based on Addition

Stepan Ivasiev
Department of cyber security
Ternopil National Economic University
Ternopil, Ukraine
isv@tneu.edu.ua

Mykhailo Kasyanchuk
Department of cyber security
Ternopil National Economic University
Ternopil, Ukraine
kasyanchuk@ukr.net

Igor Yakymenko
Department of cyber security
Ternopil National Economic University
Ternopil, Ukraine
iyakymenko@ukr.net

Oksana Gomotiuk
Department of document studies, information activity and Ukrainian studies, Ternopil National Economic University,
Ternopil, Ukraine
oksana_homotuk@ukr.net

Inna Shylinska
Department of foreign Languages and ICT,
Ternopil National Economic University
Ternopil, Ukraine
shylinska@tneu.edu.ua

Lesia Bilovus
Department of document studies, information activity and Ukrainian studies, Ternopil National Economic University
Ternopil, Ukraine
Lesya_Bilovus@i.ua

***Abstract*— This paper deals with algorithmic support for Rabin cryptosystem implementation based on addition without performing computationally expensive arithmetic operations. Due to this, there is a reduction in time and hardware complexity of the encryption and decryption processes. The proposed approach allows us to increase the amount of input data and the size of the keys in order to improve the security of the cryptosystem not affecting its efficiency. An example of Rabin cryptosystem implementation based on addition is given.**

Keywords*— *Rabin cryptosystem, addition, prime numbers, public and private keys, encryption

I. INTRODUCTION

Nowadays, along with the increase in the amount of information transmitted through telecommunication channels, the requirements for data security [1, 2] and encryption / decryption algorithms efficiency [3-5] are also increasing. These problems cannot be solved without the use of asymmetric cryptosystems, which eliminate the main disadvantage of symmetric cryptoalgorithms, that is, a reliable key exchange channel [5-8].

The main operation of most widely-used asymmetric cryptosystems, in particular RSA, ElGamal, is modular exponentiation [9, 10]. This operation is characterized by considerable time complexity, which leads to a decrease in efficiency when implementing asymmetric cryptoalgorithms [11, 12]. A modular squaring operation is used in Rabin cryptosystem to generate encrypted text, which significantly speeds up the encryption process not affecting the security of the cryptosystem in comparison with other asymmetric cryptoalgorithms [13, 14]. Rabin cryptosystem resistance to hacking, in addition to factorization [15], is also based on finding quadratic residues. Both procedures are characterized by sub-exponential time complexity [16].

One of the drawbacks of Rabin cryptosystem is the need for decimal number recovery from its residues based on the Chinese Remainder Theorem (CRT). The basic operations of the latter are quite cumbersome transformations and slow down the speed of data decryption [17, 18]. Therefore, the development of algorithmic support for implementing the Rabin cryptosystem based on new approaches that reduce the time complexity of cryptographic transformation by replacing computationally expensive arithmetic operations with the addition operation [19] is an urgent task.

II. CLASSICAL RABIN CRYPTOSYSTEM

To generate keys in Rabin cryptosystem, two arbitrary multiple-digit primes p and q are selected, which will be a secret key. Their product $n=p\cdot q$ is the public key. Encryption process of the message M (plaintext) is as follows:

$$C = M^2 \bmod n. \tag{1}$$

For the decryption of cryptogram C, additional auxiliary values f and s:

$$f = C \bmod p;\ s = C \bmod q \tag{2}$$

Then, it is necessary to find the quadratic residues modulo p and q:

$$x^2 \bmod p = f\ , \tag{3}$$

$$y^2 \bmod q = s\ . \tag{4}$$

As a result, we receive four systems of comparisons:

$$\begin{cases} M_1 \bmod p = x; \\ M_1 \bmod q = y; \end{cases} \begin{cases} M_2 \bmod p = x; \\ M_2 \bmod q = q - y; \end{cases}$$
$$\begin{cases} M_3 \bmod p = p - x; \\ M_3 \bmod q = y; \end{cases} \begin{cases} M_4 \bmod p = p - x; \\ M_4 \bmod q = q - y. \end{cases} \tag{5}$$

It should be noted that in order to find all the solutions to four systems (5) based on CRT, it is sufficient to find only two of them, for example, M_1 та M_2. Other solutions are found due to the expression $M_{3,4}=n-M_{1,2}$. One of these four solutions will be the sought message M.

This paper provides algorithmic support for all Rabin cryptosystem operations using only the addition operation.

III. ALGORITHMIC AND MATHEMATICAL SUPPORT FOR RABIN CRYPTOSYSTEM BASED ON ADDITION

To reduce the time complexity of Rabin cryptosystem for key generation and encryption, it is proposed to use the vector-modular method [9]. In particular, one of the selected numbers p and q (for example, p) is written in a binary form: $p = \sum_{i=0}^{k-1} p_i \cdot 2^i$, where k is its bitness, p_i=0 or 1. Then the row vectors $q_i=2\cdot q_{i-1}=2^i q_0$, $q_0=q$ are formed (Table 1).

TABLE I. REPRESENTATION OF ROW VECTORS FOR MULTIPLICATION

i	k-1	…	2	1	0
p_i	p_{k-1}	…	p_2	p_1	p_0
$q_i=2\cdot q_{i-1}$	q_{k-1}	…	q_2	q_1	$q_0=q$

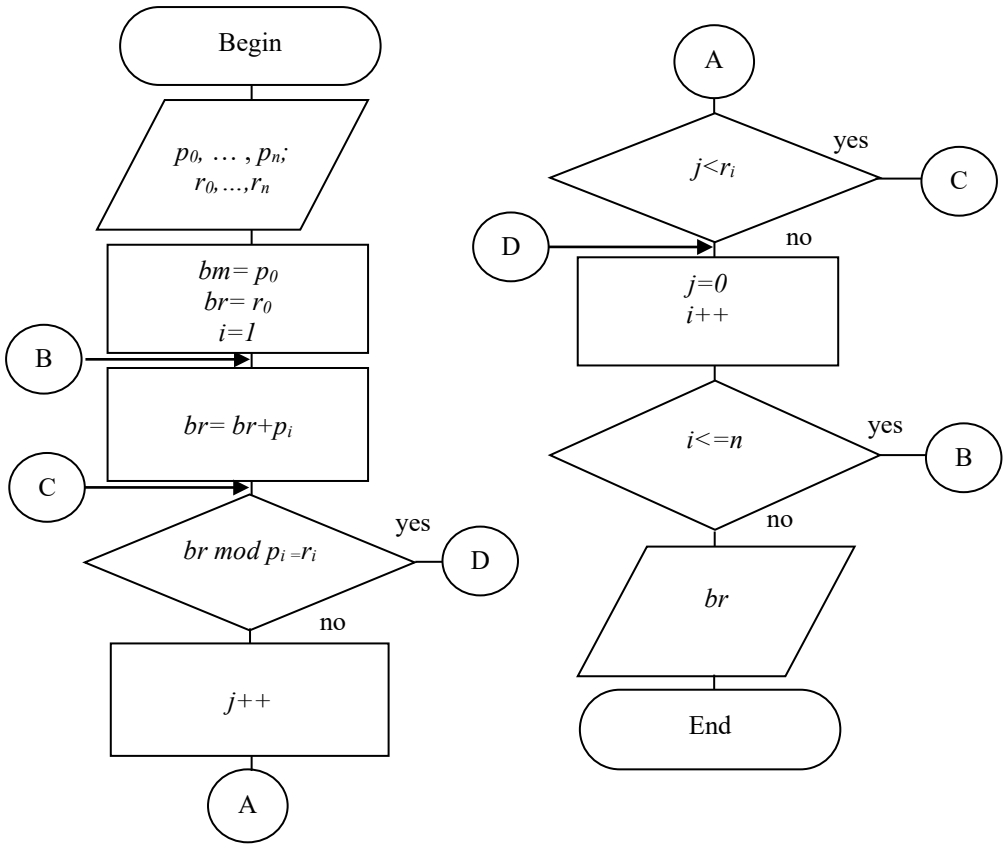

Fig. 1. A block diagram of decimal number recovery from its residues based on addition

The result of multiplication $n=p\cdot q$ is determined according to the following formula:

$$n = p \cdot q = \sum_{i=0}^{k-1} p_i \cdot q_i \qquad (6)$$

Therefore, the multiplication operation is replaced by the operation of adding those q_i, for which $p_i=1$.

Table 2 is similarly constructed for encryption according to (1). The number M is written in a binary form $M = \sum_{i=0}^{k-1} d_i \cdot 2^i$ (d_i=0 or 1) and row vectors $m_i = 2 \cdot m_{i-1} \bmod n$, $m_0=M$ are formed.

TABLE II. REPRESENTATION OF ROW VECTORS FOR MODULAR MULTIPLICATION

i	k-1	…	2	1	0
d_i	d_{k-1}	…	d_2	d_1	d_0
$m_i=2\cdot m_{i-1} \bmod n$	m_{k-1}	…	m_2	m_1	$m_0=M$

The encryption result is found according to the following formula:

$$C = M^2 \bmod n = \left(\sum_{i=0}^{k-1} d_i \cdot m_i \right) \bmod n \qquad (7)$$

Correspondingly, the operation of modular multiplication (squaring) is replaced by the operation of modular addition of those m_i, for which the corresponding d_i are equal to 1.

To find the residue of a mod n [20], k-bit number a must be written in the binary number system $a = \sum_{i=0}^{k-1} a_i \cdot 2^i$ (a_i=0 or 1) and row vectors $a_{1i}=2^i \bmod n$, i=0, …, k-1 must be created (see Table 3).

TABLE III. FINDING THE RESIDUE OF A MOD P.

i	k-1	k-2		2	1	0
a_i	a_{k-1}	a_{k-2}	…	a_2	a_1	a_0
$2^i \bmod n$	$2^{k-1} \bmod n$	$2^{k-2} \bmod n$		$2^2 \bmod n$	$2^1 \bmod n$	$2^0 \bmod n$
a_{1i}	$a_{1\,k-1}$	$a_{1\,k-2}$	…	a_{12}	a_{11}	a_{10}

The result is found according to the following expression:

$$a \bmod p = \left(\sum_{i=0}^{k-1} \left(a_i 2^i \bmod n \right) \right) \bmod n = \left(\sum_{i=0}^{k-1} \left(a_i a_{1i} \right) \right) \bmod n . \qquad (8)$$

Table 3 and expression (8) show that the sought residue will be equal to the sum of the powers of two (or a_{1i}) for which correspondingly a_i=1.

It should also be noted that two consecutive values of a_{1i} and $a_{1\,i+1}$ are defined by the following recurrence relation:

$$a_{1i+1} = \begin{cases} 2 \cdot a_{1\,i}, & 2 \cdot a_{1\,i} < n \\ 2 \cdot a_{1\,i} - p, & 2 \cdot a_{1\,i} \geq n. \end{cases} \qquad (9)$$

Figure 1 shows a block diagram of decimal number recovery from its residues based on addition. Therefore, to find the residue modulo, it is not necessary to perform a computationally expensive operation of division with remainders, but it can only be restricted to subtraction. In addition, multiplication by 2 is very simply implemented by hardware by writing zero at the end of the binary number [21, 22].

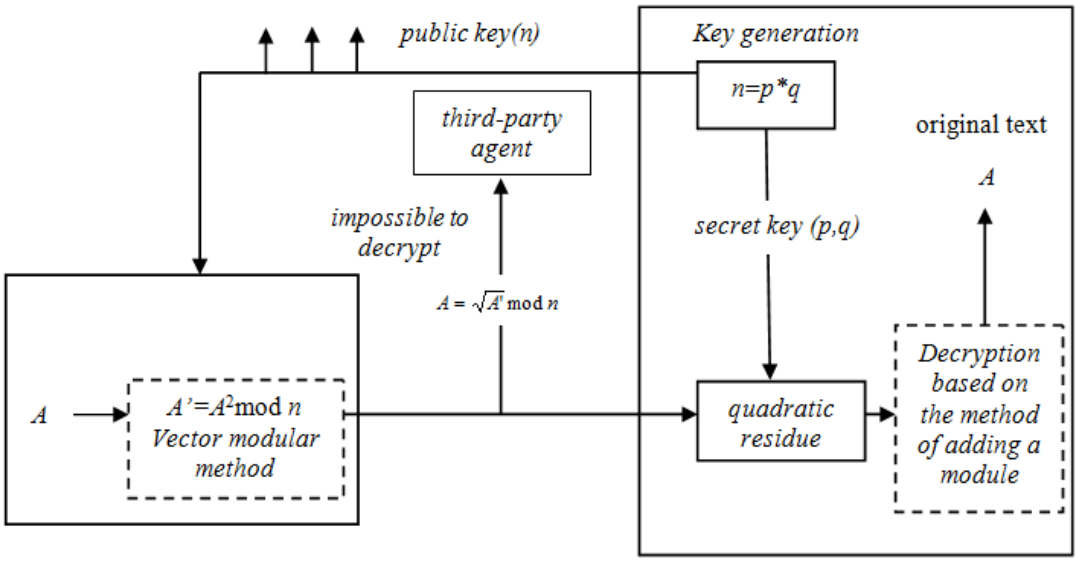

Fig. 2. A scheme of Rabin cryptosystem implementation using the method of adding a module

To find x and y in (3) - (4), it is necessary to find a square root modulo. Classical approaches using Jacobi or Legendre symbols are time consuming [23, 24]. Therefore, we propose a method that only requires addition and validation operation to see if the number is perfect square that significantly reduces the time complexity of the Rabin method. Thus, in order to find a value $x \bmod p = \sqrt{f}$, the following sequence of operations $f+p, f+2p, \ldots, f+i \cdot p$ should be performed, where i- is a value when the number $f+i \cdot p$ is perfect square. Similarly $y^2 \bmod q = s$ is found.

To find solutions to systems (5), it is suggested to use the method of adding a module. For an example, let us consider the first system of comparisons (5). Since any congruence $M_1 \bmod p=x$ can be represented as $M_1 = \lambda p + x$, де $\lambda = 0, 1, 2, \ldots$, then p module must be added to x remainder until the congruence $(x+\lambda p) \bmod q=M_1 \bmod q=y$ is performed.

Figure 2 shows the corresponding scheme of implementation of Rabin cryptosystem using this method.

It should be noted that in classical methods, in particular CRT and Garner's algorithm, it is necessary to find the modular inverse, which is accompanied by a large computational complexity [25-27] and, accordingly, leads to a deterioration of time characteristics when implementing the Rabin cryptoalgorithm.

IV. EXAMPLE OF RABIN CRYPTOSYSTEM IMPLEMENTATION BASED ON ADDITION

Let private keys be $p=37$, $q=43$, then according to (6) and Table 1 we receive $n=p \cdot q=37 \cdot 43=1376+172+43=1591$ (Table 4).

TABLE IV. SEARCH FOR PRODUCT $N=P \cdot Q$ =31·47

i	5	4	3	2	1	0
p_i	1	0	0	1	0	1
$q_i=2 \cdot q_{i-1}$	1376	688	344	172	86	43

Let plaintext M=155. Table 5 is created on the basis of formulas (1), (7) and Table 2.

TABLE V. ENCRYPTION PROCEDURE.

i	7	6	5	4
d_i	1	0	0	1
$m_i=2 \cdot m_{i-1} \bmod n$	748	374	187	889
i	3	2	1	0
d_i	1	0	1	1
$m_i=2 \cdot m_{i-1} \bmod n$	1240	620	310	155

Then we receive value $C = 155^2 \bmod 1591=(748+889+1240+310+155) \bmod 1591=3342 \bmod 1591$ is received. The result is determined according to Table 3 and (8) (Table 6).

TABLE VI. FINDING RESIDUE 3342 MOD 1591

i	11	10	9	8	7	6
a_i	1	1	0	1	0	0
a_{1i}	457	1024	512	256	128	64
i	5	4	3	2	1	0
a_i	0	0	1	1	1	0
a_{1i}	32	16	8	4	2	1

Then $3342 \bmod 1591=(457+1024+256+8+4+2) \bmod 1591=1751 \bmod 1591$. Performing normal subtraction it can be found that encrypted message C=1751-1591=160.

When decrypting cryptogram C, the expressions (2) - (4) are used: $f=160 \bmod 43=31$, $s=160 \bmod 37=12$, and the residue can be found according to Table 3 and expression (8). Then, sequences are formed where perfect square is found.

Thus, $\sqrt{31}(\bmod 43) = 17$ and 43-17=26; $\sqrt{12}(\bmod 37) = 7$ and 37-7=30. Then it is possible to form four pairs of numbers: (26, 7), (26, 30), (17, 7), (17, 30), which determine the corresponding systems of congruences:

$$\begin{cases} M_1 \bmod 43 = 26; \\ M_1 \bmod 37 = 7; \end{cases} \begin{cases} M_2 \bmod 43 = 26; \\ M_2 \bmod 37 = 30; \end{cases} \begin{cases} M_3 \bmod 43 = 17; \\ M_3 \bmod 37 = 7; \end{cases}$$

$$\begin{cases} M_4 \bmod 43 = 17; \\ M_4 \bmod 37 = 30. \end{cases} \quad (10)$$

According to the method of adding a module, the solutions of the first two systems can be conveniently presented as a

single table. In particular, the module 43 must be sequentially added to the residue 26 until the residue of the received sum modulo 37 is 7 and 30 (Table 7).

TABLE VII. PROCEDURE OF DECRYPTION

λ	0	1	2	3	4
26+43·λ	26	69	112	155	198
(26+43·λ)mod 37	26	32	1	7	13
λ	5	6	7	8	9
26+43·λ	241	284	327	370	413
(26+43·λ)mod 37	19	25	31	0	6
λ	10	11	12	13	
26+43·λ	456	499	542	585	
(26+43·λ)mod 37	12	18	24	30	

Therefore, according to Table 7, the solutions to the systems (10) are values M_1=155 (plaintext), M_2=585, M_3=1591-155=1436, M_4=1591-585=1006, which are obtained without cumbersome procedures of modular multiplication and exponentiation, CRT, quadratic residue and inverse finding based on Extended Euclidean algorithm, and the need to control the overflow of the bit grid when performing intermediate calculations.

V. CONCLUSIONS

The paper presents theoretical foundations and algorithmic support for Rabin cryptosystem implementation, in which all computationally expensive arithmetic operations (multiplication, modular squaring, finding the square root modulo, and decimal number recovery from its residues) are performed only with the use of addition. This allows reducing the time and hardware complexity of processing data in Rabin cryptosystem, increasing the unit of plaintext and the size of the keys not affecting the efficiency, and avoiding control over the overflow of the bit grid. An example of Rabin cryptosystem implementation based on addition is given.

REFERENCES

[1] Adki V., Hatkar S. A Survey on Cryptography Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2016. Vol. 6 (6). P. 469-475.

[2] Andrijchuk V.A., Kuritnyk I.P., Kasyanchuk M.M., Karpinski M.P. Modern Algorithms and Methods of the Person Biometric Identification. *Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications* (*IDAACS–2005*): Proceedings of the Third IEEE Workshop. Sofia, Bulgaria. 2005. P.403–406.

[3] Deryabin M., Chervyakov N., Tchernykh A., Babenko M., Shabalina M. High Performance Parallel Computing in Residue Number System. *International Journal of Combinatorial Optimization Problems and Informatics*. 2018. Vol. 9 (1). P. 62-67.

[4] A. Okeyinka, "Computational Speeds Analysis of RSA and ElGamal Algorithms", Proceedings of the World Congress on Engineering and Computer Science (WCECS 2015), San Francisco (USA), V. I, pp. 237-242, 2015.

[5] W. Stallings, Cryptography and Network Security: Principles and Practice, 5th Prentice Hall Press Upper Saddle River, NJ, USA, 2010, 719 p.

[6] Menezes A., van Oorschot P., Vanstone S. Handbook of Applied Cryptography. — CRC Press, 2003. — 780 p.

[7] Amalraj A. J., Raybin Jose J. J. A survey paper on cryptography techniques International Journal of Computer Science and Mobile Computing. Vol. 5, Issue. 8, 2016, pp.55 – 59.

[8] Valarmathy N., Vishnupriya P. Network Security and Cryptography Techniques. Networkihg and Communication Engineering. 2017. Vol.9, №9. Pp. 229-231.

[9] Yakymenko I.Z., Kasianchuk M.M., Ivasiev S.V., Melnyk A.M., Nykolaichuk Ya.M. Realization of RSA cryptographic algorithm based on vector-module method of modular exponention. *Modern Problems of Radio Engineering, Telecommunications and Computer Science* (*TCSET–2018*): Proceedings of the XIV–th International Conference. L'viv–Slavske. 2018. P.550-554.

[10] Song Y. Cryptanalytic attacks on RSA. Springer Science and Business Media, Inc., 2008. 255 p.

[11] Yakymenko I., Kasyanchuk M., Nykolaychuk Ya. Matrix Algorithms of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestenson's Basis. *Modern Problems of Radio Engineering, Telecommunications and Computer Science* (*TCSET–2010*): Proceedings of the X–th International Conference. L'viv–Slavske. 2010. P.241.

[12] Shoup V. A Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2005. 517 p.

[13] Arpit K., Mathur A. "The Rabin cryptosystem and analysis in measure of chinese reminder theorem" Int. J. Sci. Res. Public. — 2013. — V.3. — P. 1–4.

[14] Hayder R.H. H-Rabim Cryptosystem. *Journal of Mathematics and Statistics*. 2014. Vol. 10 (3). P. 304-308.

[15] Karpiński M., Ivasiev S., Yakymenko I., Kasianchuk M., Gancarczyk T. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes // Proc. of 16th International Conference on Control, Automation and Systems (ICCAS–2016). — Gyeongju, Korea. — V.1. — October, 2016. — P.1484–1486.

[16] Kasianchuk M., Yakymenko I., Pazdriy I., Melnyk A., Ivasiev S. "Rabin's modified method of encryption using various forms of system of residual classes", Proceedings of the XIV International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2017). — Polyana-Svalyava (Zakarpattya), Ukraine. — 2017. — P.222-224.

[17] Srivastava A., Mathur A. The Rabin cryptosystem and analysis in measure of chinese reminder theorem. *International Journal of Scientific and Research Publications*. 2013. Vol. 3 (6). P. 1-4.

[18] Dasgupta S., Papadimitriou C., Vazirani U. Algorithms. — McGraw-Hill Science, Engineering, 2006. — 336 p.

[19] Karpinski M., Rajba S., Zawislak S., Warwas K., Kasianchuk M., S. Ivasiev, I. Yakymenko A Method for Decimal Number Recovery from its Residues Based on the Addition of the Product Modules // Proceedings of the 10th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2019). — 2019.— V.1. — P.13–17.

[20] Ivasiev S., Yakymenko I., Kasianchuk M., Shevchuk R., Karpinski M., Gomotiuk O. Effective algorithms for finding the remainder of multi-digit numbers. *Advanced Computer Information Technology* (*ACIT–2019*): Proceedings of the International Conference. Ceske Budejovice (Czech Republic). 2019. P. 175-178.

[21] Beuchat J.-L. Some Modular Adder and Multipliers for Field Programmable Gate Arrays. *Parallel and Distributed Processing:* IEEE Proceedings of International Symposium. 2010. Vol.17. P.8-11.

[22] Wu H. Bit-Parallel Finite Field Multiplier and Squarer Using Polynomial Basis. *IEEE Transactions on Computers*. 2002. Vol.51 (7). P. 151-155.

[23] Hardy G.H., Wright E.M., Wiles A. An Introduction to the Theory of Numbers. Oxford University Press, 2008. 656 p.

[24] Jeffrey H., Jill P., Joseph H. An Introduction to Mathematical Cryptography. Berlin: Springer, 2008. 540 p.

[25] Zhengbing Hu., Dychka I., Onai M., Bartkoviak A. The Analysis and Investigation of Multiplicative Inverse Searching Methods in the Ring of Integers Modulo M. *International Journal of Intelligent Systems and Applications (IJISA)*. 2016. Vol. 8, №11. P. 9-18.

[26] Rajba T. Klos-Witkowska A., Ivasiev S., Yakymenko I., Kasianchuk M. Research of Time Characteristics of Search Methods of Inverse Element by the Module. Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2017): Proceedings of the 2017 IEEE 9th International Conference. Bucharest, Romania. V.1. September, 2017. P.82–85.

[27] Parthasarathy S. Multiplicative inverse in mod(m). *Algologic Technical Report*. 2012. №1. P. 1-3.