Conference Program

15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET - 2020)

in partnership with

Lviv-Slavske, Ukraine
February 25-29, 2020

ORGANIZERS

- IEEE Ukraine Section
- IEEE MTT/ED/AP/EP/SSC Joint West Ukraine Chapter
- Lviv Polytechnic National University, Ukraine
- Military University of Technology, Poland

CONFERENCE HONORARY CHAIR

Yuriy Bobalo, Rector of Lviv Polytechnic National University

ORGANAZING COMMITTEE

CHAIR

Prof. Ivan Prudyus, Lviv Polytechnic National University

CHAIR'S DEPUTIES

Prof. Marek Kuchta, Military University of Technology

Prof. Myroslav Kiselychnyk, Lviv Polytechnic National University

CONFERENCE SECRETARY

Assoc. Prof. Leonid Ozirkovskyy, Lviv Polytechnic National University

PUBLICATION CHAIR

Prof. Orest Lavriv, Lviv Polytechnic National University

CONFERENCE TREASURER

Assist. Prof. Sergiy Fabirovskyy, Lviv Polytechnic National University

MEMBERS

Prof. Berkman L., (Kyiv, Ukraine)
PhD. Beshley M., (Lviv, Ukraine)
Prof. Bezruk V., (Kharkiv, Ukraine)
Assoc. Prof. Fast V., (Lviv, Ukraine)
PhD Hnilitskyi Y., (Lviv, Ukraine)
Assoc. Prof Korzh R., (Lviv, Ukraine)
Prof. Kychak V., (Vinnytsya, Ukraine)
Assist. Prof. Kulyk I., (Lviv, Ukraine)
Prof. Lozhkovskyy A., (Odesa, Ukraine)
PhD Maksymiuk T., (Lviv, Ukraine)
Prof. Mosorov V., (Lodz, Poland)
Prof. Pavlysh V., (Lviv, Ukraine)
Prof. Politanskyy L., (Chernivtsi, Ukraine)
Prof. Semenko A., (Kyiv, Ukraine)
PhD Shpur O., (Lviv, Ukraine)
Sen. Researcher Tkachenko V., (Lviv, Ukraine)
Prof. Uryvskyy L., (Kyiv, Ukraine)
PhD Zmysnyi M., (Lviv, Ukraine)

CONFERENCE SECTIONS

Section ID	Section Title	Number of accepted papers
S0	Plenary Session	8
S1	Antennas, microwave technology, electromagnetic compatibility, radar systems, satellite communication, monitoring and positioning systems	18
S2	Information systems and technologies, computer-aided design	18
S3	Electronic circuits and signals, simulation of electro-technical and electro-energetic systems	27
S4	Electronics, photonics and innovative optical technologies: systems and devices, micro- and nanotechnologies	24
S5	Cybersecurity in ICT	19
S6	Internet of Things and biomedical engineering	19
S7	Information processing	18
S8	Telecommunications: wired and wireless systems, network services, simulation and management	30
S9	Models, algorithms, software and hardware construction means of information and communication, radio electronic devices and systems	30
	ACCEPTED PAPERS, TOTAL	216
	SUBMITTED PAPERS, TOTAL	282
	ACCEPTANCE RATE	0,77

TIME LIMITS

Plenary session: up to 25 min	**Regular sessions:** up to 15 min

POSTER SESSION

1.	*Dawei Dong, Ye Zhiwei, Jun Su, Shiwei Xie, Yu Cao and Roman Kochan* **A Malware Detection Method Based on Improved Fireworks Algorithm and Support Vector Machine**
2.	*Stepan Ivasiev, Ihor Yakymenko, Mykhailo Kasianchuk, Oksana Gomotiuk, Grygorii Tereshchuk and Pavlo Basistyi* **Elgamal cryptoalgorithm on the basis of the vectormodule method of modular exponentiation and multiplication**
3.	*Volodymyr Maksymovych and Andrii Malohlovets* **Design and FPGA prototype of modified Blum-Blum-Shub pseudorandom sequence generator**
4.	*Oleksii Bychkov, Kateryna Merkulova and Yelyzaveta Zhabska* **Information Technology of Person's Identification by Photo Portrait**
5.	*Mykola Kushnir, Hryhorii Kosovan, Petro Krojalo and Andrii Komarnytskyy* **Encryption of the images on the basis of two chaotic systems with the use of fuzzy logic**
6.	*Yuliia Pyrih, Mykola Kaidan, Bohdan Strykhalyuk and Viktoriia Zhebka* **A Modified Simulated Annealing Algorithm Based on Principle of the Greedy Algorithm for Networks with Mobile Nodes**
7.	*Petro Snitsarenko, Oleksii Zahorka, Andrii Koretskyi, Yurii Sarychev and Volodymyr Tkachenko* **Expert methods application to assess information security threats impact in the military sphere**

Elgamal cryptoalgorithm on the basis of the vector-module method of modular exponentiation and multiplication

Ihor Yakymenko
Department of cybersecurity
Ternopil National Economic University,
Ternopil, Ukraine
iyakymenko@ukr.net

Mykhailo Kasianchuk
Department of cybersecurity
Ternopil National Economic University,
Ternopil, Ukraine
kasyanchuk@ukr.net

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

Grygorii Tereshchuk
Department of technological education and labor protection
Ternopil Volodymyr Hnatiuk National Pedagogical University
Ternopil, Ukraine
g.tereschuk@tnpu.edu.ua

Stepan Ivasiev
Department of cybersecurity
Ternopil National Economic University,
Ternopil, Ukraine
stepan.ivasiev@gmail.com

Pavlo Basistyi
Department of physics
Ternopil Volodymyr Hnatiuk National Pedagogical University
Ternopil, Ukraine
basi@ukr.net

***Abstract*— This paper presents the implementation of the ELGamal cryptoalgorithm for information flows encryption / decryption, which is based on the application of the vector-modular method of modular exponentiation and multiplication. This allows us to replace the complex operation of the modular exponentiation with multiplication and the last one with addition that increases the speed of the cryptosystem. In accordance with this, the application of the vector-modular method allows us to reduce the modular exponentiation and multiplication temporal complexity in comparison with the classical one.**

***Keywords*—ElGamal cryptosystem, vector-modular method, exponentiation, multiplication, temporal complexity.**

I. Introduction

Today asymmetric cryptographic algorithms RSA [1, 2], ElGamal [3] and Rabin [4] are the most common to provide a high level of information stream protection [5, 6]. Their main operations are modular exponentiation (ME) and modular multiplication (MM) of multi-digit numbers [7-9,]. Parameters of the specified asymmetric cryptosystems (keys, encryption block and cryptographic transformation module) must be at least 1024 bits with a growth perspective in the years to 2048 and 4096 bits. However, the most binary-decimal system of number is common in modern computing systems and has certain functional limitations [10-12], which inevitably leads to deterioration of the temporal characteristics of the algorithms [13].

The use of various forms of the Residue number system (RNS) [14-17] and vector-modular methods (VMM) of MM and ME [18] is one of the ways to increase the speed of asymmetric cryptographic algorithms. In particular, a three-module crypto Rabin algorithm is developed in [19] using the usual integer and modified perfect RNS forms, which has the advantage of resilience to the classical Rabin cryptosystem by increasing the block of open text for encryption. Implementation of the crypt algorithm RSA is presented in [20] on the basis of the use of the VMM of ME. This fact made it possible to replace computationally complex arithmetic operations with an addition operation, which increases the performance of the RSA cryptosystem. Therefore, The purpose of this work is to implement the ElGamal algorithm for encoding on the basis of the VMM of ME and MM, which allows you to calculate the numbers of lesser digit than the classical approach and reduce the time complexity of the basic operations of the cryptographic algorithm.

II. ElGamal encryption scheme

A large prime number p is chosen to encrypt the open text block M in the ElGamal cryptosystem and all operations in the field (or in the multiplicative group) by module of number p are considered [21]. The random number $1<q<p$, which is the generator of the multiplicative group (element, which, in ME, forms all elements of the group in all degrees) is chosen. In this case, all numbers that are mutually-prime conjoin with p,

will be generators. Next, selecting the power index $2<x<p$-1, the number y is calculated:

$$y = q^x \bmod p. \quad (1)$$

Then the open key will be the set (y, q, p), and the closed – number x. The complexity of recovering a private key from the open is related to the problem of a discrete logarithm [22]. This task is as complex as factorization [23-24]. At present, there are no effective polynomial algorithms for calculating the number of x, although there are sub-exponential algorithms and algorithms for a quantum computer that, for a certain bit of input parameters, can solve this problem. The auxiliary random number $1<k<p$-1 is introduced for encryption in the ElGamal scheme and two numbers of a and b, which are blocks of encrypted text are calculated:

$$a = q^k \bmod p,\ b = y^k \cdot M \bmod p. \quad (2)$$

Consequently, in the ElGamal scheme, the size of the encrypted message is always twice as large as the size of the open text. Decryption occurs according to this expression:

$$M = b \cdot (a^x)^{-1} \bmod p. \quad (3)$$

It should be noted that the following formula is more suitable for practical calculations:

$$M = b(a^x)^{-1} \bmod p = ba^{p-1-x} \bmod p \quad (4)$$

Since a random variable is introduced into the ElGamal scheme, it is probabilistic or it is also called a cipher of multivalued replacement. They have greater resistance to cryptanalysis compared to schemes with a certain encryption process. The disadvantage of the ElGamal crypt algorithm is the doubling of the length of the encrypted text compared with the original.

III. Teoretical bases of the VMM

As we noted above, the basic arithmetic operations of the ElGamal cryptosystem are MM and ME. The exponent of extend must be written in degrees of two to perform ME in the generation of keys in accordance with expression (1) and use the following ratio:

$$y = q^x \bmod p = \left(\prod_{i=0}^{n-1} q^{\sum_{i=0}^{n-1} x_i 2^i} \right) \bmod p = \prod_{i=0}^{n-1} r_i \bmod p. \quad (5)$$

where n – bit capacity of the module p, x_i=0 or 1, $r_i = q^{2^i} \bmod p$, moreover $r_i = (r_{i-1})^2 \bmod p$.

The result can be obtained by multiplying the values r_i, for which the corresponding x_i=1 (Table 1).

TABLE I. Vector-Modular Method of Modular Exponentiation

i	n-1		3	2	1	0
x_i	x_{n-1}	...	x_3	x_2	x_1	x_0
$r_i = q^{2^i} \bmod p$	r_{n-1}	...	r_3	r_2	r_1	r_0

The main advantages of the proposed method is to perform operations on numbers of smaller sizes, which allows to accelerate the ME algorithm.

When finding a product $r_i r_{i-1} \bmod p$, multipliers must be represented as follows: $r_i = \sum_{j=0}^{n-1} l_j \cdot 2^j$ and $r_{i-1} = \sum_{c=0}^{n-1} w_c \cdot 2^c$, where $l_j, w_c = 0,1$. Next, two vector-lines are constructed, in the first of which the elements are written, $h_0 = 2^0 r_i \bmod p$, $h_i = 2 \cdot h_{i-1} \bmod p$, in the second w_i (Table 2).

TABLE II. Representation of Vector-Lines of Modular Multiplication

i	n-1	…	2	1	0
w_i	w_{n-1}	…	w_2	w_1	w_0
$h_i = 2 \cdot h_{i-1} \bmod p$	h_{n-1}	…	h_2	h_1	$h_0 = 2^0 \cdot r_i \bmod p$

The result of the MM of two n – bit capacities of numbers:

$$r_i r_{i-1} \bmod p = \left(\sum_{i=0}^{n-1} w_i \cdot h_i \right) \bmod p. \quad (6)$$

Consequently, the operation of MM is replaced by the modular addition of those h_i, for which the corresponding w_i is equal to 1. This method is characterized by less time complexity compared with the classical ones. The encryption and decryption operations, which, according to expressions (2) and (4), are reduced to ME and MM, are performed analogously on the basis of the VMM.

IV. Example of realization of the ElGamal crypt algorithm on the basis of the VMM of ME and MM

The example of encryption / decryption using the ElGamal algorithm is presented. At the begining, private and public keys are generated. Let p = 29, q = 19. x = 21 – a random integer is selected for which the inequality $1<x<p$ is true. On the basis of the VMM of ME, the parameter $x = 21$ is written in degrees 2 and the value is calculated:

$$y = q^x \bmod p = 19^{21} \bmod 29 = \left(19^{(1 \cdot 2^0 + 1 \cdot 2^2 + 1 \cdot 2^4)} \right) \bmod 29. \quad (7)$$

The search procedure and the result (y = 17) are presented in Table 3. So, (p, q, y)=(29, 19, 17) will be the public key, and x=21 will be private. Next you need to select the random integer 1<k<p-1. Let k=23. Then, on the basis of a VMM of ME, having written 23 by degrees 2 and the parameter a is calculated:

$$a = q^k \bmod p = 19^{23} \bmod 29 = \left(19^{(1\cdot 2^0+1\cdot 2^1+1\cdot 2^2+1\cdot 2^4)}\right) \bmod 29 . \quad (8)$$

The search procedure and the result (a = 18) are presented in Table 4. To encrypt the open text M=14, the number 23 is written in degrees 2 and according to (2) the following expression is obtained:

$$b = M \cdot y^k \bmod p = \left(14 \cdot 17^{23}\right) \bmod 29 = \\ = \left(14 \cdot 17^{(1\cdot 2^0+1\cdot 2^1+1\cdot 2^2+1\cdot 2^4)}\right) \bmod 29. \quad (9)$$

The search procedure and the result (b = 23) are presented in Table 5. The resulting pair (a, b) = (18,23) is a cipher text.

The search procedure and the result (M=14) are presented in Table 6. Decryption occurs according to formula (4), having written the power index in degrees 2:

$$M = b \cdot (a^x)^{-1} \bmod p = b \cdot a^{p-1-x} \bmod p = \\ = 23 \cdot 18^7 \bmod 29 = 23 \cdot 18^{(1\cdot 2^0+1\cdot 2^1+1\cdot 2^2)} \bmod 29. \quad (10)$$

Consequently, this approach, which is based on the use of the VMM of ME and MM in encryption / decryption tasks based on the asymmetric ElGamal cryptosystem, can reduce the time complexity of the basic operations by replacing the exponentiation operation with the multiplication operation, and multiplication by the addition.

V. CONCLUSIONS

The implementation of the ElGamal encryption algorithm, which is based on VMM ME and MM, allows us to accelerate the procedure of data processing by replacing the ME with MM operation and multiplication with the modular addition operation. This approach provides unique opportunities for implementation of reliable and efficient cryptographic algorithms by increasing the dimension of the input parameters (message size, key), which leads to increase in stability of the considered cryptosystem. Application of the proposed approach to the ElGamal cryptosystem is shown.

TABLE III. PUBLIC KEY SEARCH

i	4	3	2	1	0
$21_{(10)}=10101_{(2)}$	1	0	1	0	1
$19^{2^i} \bmod 29$	$19^{2^4} \bmod 29 = 16$	$19^{2^3} \bmod 29 = 25$	$19^{2^2} \bmod 29 = 24$	$19^{2^1} \bmod 29 = 13$	$19^{2^0} \bmod 29 = 19$
$19^{21} \bmod 29$	19·24·16 mod 29				
2^i·24 mod 29	7	18	9	19	24
$19_{(10)}=10011_{(2)}$	1	0	0	1	1
19·24 mod 29	(7+19+24) mod 29=21				
2^i·21 mod 29	17	23	26	13	21
$16_{(10)}=10000_{(2)}$	1	0	0	0	0
16·21 mod 29	19·24·16 mod 29=21·16 mod 29=17				

TABLE IV. PUBLIC FINDING THE NUMBER OF A

i	4	3	2	1	0
$23_{(10)}=10101_{(2)}$	1	0	1	1	1
$19^{2^i} \bmod 29$	$19^{2^4} \bmod 29 = 16$	$19^{2^3} \bmod 29 = 25$	$19^{2^2} \bmod 29 = 24$	$19^{2^1} \bmod 29 = 13$	$19^{2^0} \bmod 29 = 19$
$19^{23} \bmod 29$	19·13·24·16 mod 29=13·17 mod 29				
2^i·13 mod 29	5	17	23	26	13
$17_{(10)}=10001_{(2)}$	1	0	0	0	1
19·24 mod 29	19·13·24·16 mod 29=(5+13) mod 29=18				

TABLE V. FINDING THE NUMBER OF B

i	4	3	2	1	0
$23_{(10)}=10001_{(2)}$	1	0	1	1	1
$17^{2^i} \bmod 29$	$17^{2^4} \bmod 29 = 1$	$17^{2^3} \bmod 29 = 1$	$17^{2^2} \bmod 29 = 1$	$17^{2^1} \bmod 29 = 28$	$17^{2^0} \bmod 29 = 17$
$14 \cdot 17^{23} \bmod 29$	14·17·28·1·1 mod 29				
2^i·14 mod 29	21	25	27	28	14
$17_{(10)}=10001_{(2)}$	1	0	0	0	1
14·17 mod 29	(21+14) mod 29=6				
2^i·28 mod 29	5	17	23	26	28
$6_{(10)}=00110_{(2)}$	0	0	1	1	0
2·28 mod 29	14·17·28·1·1 mod 29=(23+26) mod 29=23				

TABLE VI. DECODING THE MESSAGE BY THE ELGAMAL SCHEME

i	4	3	2	1	0
$7_{(10)}=00111_{(2)}$	0	0	1	1	1
$18^{2^i} \bmod 29$	$18^{2^4} \bmod 29 = 24$	$18^{2^3} \bmod 29 = 16$	$18^{2^2} \bmod 29 = 25$	$18^{2^1} \bmod 29 = 5$	$18^{2^0} \bmod 29 = 18$
$23 \cdot 18^{23} \bmod 29$	$23 \cdot 25 \cdot 5 \cdot 18 \bmod 29$				
$2^i \cdot 23 \bmod 29$	20	10	5	17	23
$25_{(10)}=10001_{(2)}$	1	1	0	0	1
$23 \cdot 25 \bmod 29$	$(20+10+23) \bmod 29=24$				
$2^i \cdot 18 \bmod 29$	27	28	14	7	18
$5_{(10)}=00110_{(2)}$	0	0	1	0	1
$5 \cdot 18 \bmod 29$	$(14+18) \bmod 29=3$				
$2^i \cdot 24 \bmod 29$	7	18	9	19	24
$3_{(10)}=00011_{(2)}$	0	0	0	1	1
$3 \cdot 24 \bmod 29$	$23 \cdot 25 \cdot 5 \cdot 18 \bmod 29=3 \cdot 24 \bmod 29=(19+24) \bmod 29=14$				

REFERENCES

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

[2] Ambedkar B.R., Gupta A., Gautam P., Bedi S. An Efficient Method to Factorize the RSA Public Key Encryption. *Communication Systems and Network Technologies:* Proceeding of International Conference. 2011. P. 108–111.

[3] A.E. Okeyinka, "Computational Speeds Analysis of RSA and ElGamal Algorithms on Text Data", Proceedings of the World Congress on Engineering and Computer Science (WCECS 2015) – San Francisco, USA –V. I. – October 21-23, 2015 – P.237-242.

[4] K. Arpit and A. Mathur, "The Rabin cryptosystem and analysis in measure of chinese reminder theorem", Int. J. Sci. Res. Public., 3: 1-4, 2013, pp.380.

[5] W. Stallings, Cryptography and Network Security: Principles and Practice (7th edition). Prentice Hall, 2016, 768 p.

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

[7] Ye J., Chen X., Ma J., "An improved algorithm for secure outsourcing of modular exponentiations", 29th International Conference on Advanced Information Networking and Applications Workshops (AINA'15) – Gwangju, Korea (2015) – P. 73–76.

[8] I. Marouf, M. Mosab Asad, Q. Abu Al-Haija, "Comparative Study of Efficient Modular Exponentiation Algorithms", COMPUSOFT, An international journal of advanced computer technology, 6 (8), August-2017 – Volume VI, Issue VIII – P. 2381-2389.

[9] 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.

[10] B Krulikovskyi, N Vozna, V Kimak, and A Davletova, "The method to optimize structural, hardware and time complexities characteristics multi-bit adders of special processors for data encryption", Proceedings of the 13th International Conference on Modern Problems of Radio Engineering. Telecommunications and Computer Science (TCSET), 2016 455-459.

[11] I. Tsmots, V. Teslyuk, T. Teslyuk, and I. Ihnatyev, "Basic Components of Neuronetworks with Parallel Vertical Group Data Real-Time Processing", Advances in Intelligent Systems and Computing II. CSIT 2017. Advances in Intelligent Systems and Computing, vol. 689, Springer, Cham. – P. 558 - 576.

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

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

[14] M.N. Kasianchuk, Ya.N. Nykolaychuk, I.Z. Yakymenko, "Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes", Journal of Automation and Information Sciences. 2016, Vol.48, №8, p.56-63.

[15] V Yatskiv, T Tsavolyk, N Yatskiv, "The correcting codes formation method based on the residue number system", Proceedings of the 14th International Conference Experience of Designing and Application of CAD Systems in Microelectronics (CADSM), 2017 237-240

[16] Omondi A., Premkumar B. Residue number systems: theory and implementation. London: Imperial College Press, 2007. 296 p.

[17] Ananda Mohan P.V. Residue Number Systems: Theory and Applications. Birkhäuser, 2016. 351 p.

[18] D. Kozaczko, M. Kasianchuk, I. Yakymenko, and S.Ivasiev, "Vector Module Exponential in the Remaining Classes System", Proceedings of the 2015 IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2015) – Warsaw, Poland. – V.1. – September, 2015. – P.161–163.

[19] M. Kasianchuk, I. Yakymenko, I. Pazdriy, A. Melnyk, and S.Ivasiev, "Rabin's modified method of encryption using various forms of system of residual classes", XIV International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2017)", 21-25 February, 2017, Polyana-Svalyava (Zakarpattya), Ukraine. – P.222-224.

[20] I.Z. Yakymenko, M.M. Kasianchuk, S.V. Ivasiev, A.M. Melnyk., Y.M. Nykolaichuk, "Realization of RSA cryptographic algorithm based on vector-module method of modular exponention", 14th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, TCSET 2018 – Proceedings 2018-April, pp. 550-554.

[21] H. Hayder Raheem, N. Irtifaa, "Abdalkadum Image Encryption and Decryption in A Modification of ElGamal Cryptosystem in MATLAB", International Journal of Sciences: Basic and Applied Research (IJSBAR)(2014) –Volume 14, No 2 – P. 141-147.

[22] H. Hayder Raheem, "The Discrete Logarithm Problem in the ElGamal Cryptosystem over the Abelian Group U(n) Where n= p^m ,or $2p^m$", International Journal of Mathematics Trends and Technology – Volume 7, No 3 – March 2014 – P. 184–189.

[23] M. Karpiński, S. Ivasiev, I. Yakymenko, M. Kasianchuk, and T. Gancarczyk, „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.

[24] Somsuk K., Tientanopajai K. An Improvement of Fermat's Factorization by Considering the Last m Digits of Modulus to Decrease Computation Time. *International Journal of Network Security*. 2017. Vol.19 (1). P.99-111.