Modeling of Asymmetric Modular Encryption System

R. Biyashev, S. Nyssanbayeva, N. Kapalova, D. Dyusenbayev

Abstract **-** The encryption system with public key developed on the basis of the ElGamal cipher system and non-positional polynomial notations (NPNs) has been constructed and investigated. The software realization of this system has been realized. Work of the computer program has been checked on concrete examples. The efficiency of the realized non-positional system of encryption can significantly increase owing to the possibility of parallel processing of polynoms which are the remainders on the chosen base number system of NPNs.

Keywords— Asymmetric encryption, nonpositional polynominal notations, cryptostrength, residue.

I. INTRODUCTION

ASYMMETRIC cryptography which was invented and developed for the last decades of the last century took almost the same place during this time as block symmetric encryption running to semicentennial history. They solve those problems which are unsoluble for symmetric algorithms, but the speed of work is much lower.

Cryptographic strength of El-Gamal encryption system with public key is based on complexity of the problem of discrete logarithming in the multiplicative group of a finite field. It is difficult to realize this task for *p* values containing more than 150 decimal signs. It is recommended to choose *p* such that the number *p-1* contains a big simple divider.

The drawback of ElGamal cryptosystem is doubling of the length of a plain text when enciphering, and also the need for the use of various values of the randomizer for encryption of various plain texts [1-4]. These algorithms consume a significant amount of time and resources and calculation time for data encryption and decryption. In work [5] various experiments were conducted where it was noted that the El-Gamal scheme is slightly inferior only to RSA.

The development of cryptography is in progress – new algorithms are developed and the existing ones are modified. As practice shows , now the perspective direction in cryptography is also hybrid encryption [6].

At the Institute of Information and Computational Technologies scientific work is conducted on the development and research of symmetric and asymmetric algorithms of encryption and digital signature developed with use of the algebraic approach on the basis of non-positional polynomial notations [7-9].

Synonyms of NPNs are polynomial notations in residue classes, non-positional notations and modular arithmetic. Algorithms and methods created on the basis of these systems are also called nonconventional, non-positional or modular [6-9]. In classic residue notation (PN) only positive, pairwise prime integers are chosen as a system of base numbers, and a positive integer in such system is presented by its remainders (residues) of division by this system of base numbers [6]. Creation of RN is based on the Chinese remainder theorem use. According to this theorem, representation of a number as a sequence of residues is unique in case if base numbers are pairwise relatively primes. In contrast to classic RN in NPNs the irreducible polynomials over the field *GF* (2), i.e. those with binary coefficients, are used as base numbers [7, 8].

The peculiarity of nonconventional cryptographic algorithms is the possibility of parallelization of performance of arithmetic transactions modulo base numbers of NPNs, in this regard the speed of cryptoalgorithm performance increases.

Simultaneously with these works, researches are conducted on modification of the developed model with use of Feystel network and EDS on the basis of NPNs. For receiving the model of nonconventional algorithm of encryption on the basis of NPNs, the modified Feystel's scheme was used. The purpose of these works is the improvement of statistical

This work is financed under the scientific-technical program №0128/ PTF-14 of the Committee of Science of the Ministry of Education and Science of the Republic of Kazakhstan

Rustem Biyashev, Doctor of Technical Sciences, professor, Head of the Laboratory of Information Security of the Institute of Information and Computational Technologies of the Ministry of Education and Science of the Republic of Kazakhstan, 050010, Almaty, Pushkin Street, 125 (phone: +7 (727) -272-80-05, +7 (727) -272-37-11, fax: +7 (727) -272-37-11, e-mail: brg@ipic.kz, http//www.ipic.kz)

Saule Nyssanbayeva, Doctor of Technical Sciences, associate professor, chief research worker of the Institute of Information and Computational Technologies of the Ministry of Education and Science of the Republic of Kazakhstan, 050010, Almaty, Pushkin Street, 125 (phone: +7 (727) -272-80-05, +7 (727) -272-37-11, fax: +7 (727)-272-37-11, e-mail: sultasha1@mail.ru, http//www.ipic.kz)

Nursulu Kapalova, Candidate of Technical Sciences, leading research worker of the Institute of Information and Computational Technologies of the Ministry of Education and Science of the Republic of Kazakhstan, 050010, Almaty, Pushkin Street, 125 (phone: +7 (727) -272-80-05, +7 (727) -272-37-11, fax: +7 (727) -272-37-11, e-mail: kapalova@ipic.kz, http//www.ipic.kz)

Dilmukhanbet Dyusenbayev, software engineer of the Institute of Information and Computational Technologies of the Ministry of Education and Science of the Republic of Kazakhstan, 050010, Almaty, Pushkin Street, 125 (phone: +7 (727) -272-80-05, +7 (727) -272-37-11, fax: +7 (727) -272-37-11, e-mail: dimash_dds@mail.ru, http//www.ipic.kz)

characteristics of non-positional cryptograms. Also works are carried out on the creation of modular system of the DS with public key at whose creation the modified algorithm DSA on the basis of NPNs [10] will be used.

II. Non-Positional System of Encryption on the Basis of ElGamal Algorithm

The developed nonconventional asymmetric algorithm of encryption of electronic message *M* according to the ElGamal scheme is carried out as follows.

1. At the first stage the formation of NPNs is realized. For this purpose, irreducible polynomials are chosen as base numbers

$$p_1(x),\ p_2(x),...,\ p_S(x) \qquad (1)$$

over the field GF(2) of degree $m_1, m_2, ..., m_S$ respectively. Polynoms (1), with allowance for the order of their arrangement, form one system of base numbers. All base numbers have to be various also in case if they have one degree (for performance by the Chinese remainder theorem). The working range of NPN is defined by a polynomial (module)

$$P_S(x) = p_1(x)p_2(x)\cdots p_S(x)$$

of degree $m = \sum_{i=1}^{S} m_i$. In NPNs any polynomial $F(x)$ of degree less than *m* has the only non-positional representation of the form

$$F(x) = (z_1(x), z_2(x),..., z_S(x)), \qquad (2)$$

where $F(x) \equiv z_i(x)(\mathrm{mod}(p_i(x))$, $i = \overline{1,S}$. By the form (2), the positional representation $F(x)$ is restored as follows:

$$F(x) = \sum_{i=1}^{S} z_i(x)B_i(x)\text{, where}$$

$$B_i(x) = \frac{P_S(x)}{p_i(x)}M_i(x) \equiv 1(\mathrm{mod}\ p_i(x)). \qquad (3)$$

The choice of polynomials $M_i(x)$ is carried out in such way so that comparison in (3) is carried out.

Base numbers of NPNs are chosen so that their total length m consists the length of the message or its block.

2. For every base number $p_i(x)$ the generating element (polynomial) $\alpha_i(x)$ is chosen from the complete residue system modulo $p_i(x)$, i.e. degrees $\alpha_i(x)$ don't exceed m_i, where $i = \overline{1,S}$.

Then the generating element in nonconventional algorithm of encryption is interpreted as a sequence of remainders of division of some polynomial $\alpha(x)$ by base numbers $p_1(x), p_2(x),..., p_S(x)$ respectively:

$$\alpha(x) = (\alpha_1(x), \alpha_2(x),..., \alpha_S(x))\ ,$$

where $\alpha(x) \equiv \alpha_i(x)(\mathrm{mod}\ p_i(x))$, $i = \overline{1,S}$.

The chosen base numbers of NPNs and the generating polynomials $\alpha_i(x)$ corresponding to them are kept as a secret. The generating element is the analog of the primitive element of primitive root modulo a prime number.

For restoration of the result in the positional form by its remainders the bases of NPNs are determined by formula (3). For this purpose, polynomials are calculated

$$\delta_i(x) \equiv \frac{P_S(x)}{p_i(x)}(\mathrm{mod}\ p_i(x))$$

and polynoms, inverse to them

$$\delta_i^{-1}(x)\cdot\delta_i(x) \equiv 1(\mathrm{mod}\ p_i(x)).$$

Then the bases are found by the formula

$$B_i(x) = \delta_i^{-1}(x)\cdot\frac{P_S(x)}{p_i(x)},$$

and they are also the confidential parameters of the algorithm.

3. Then users *A* and *B* independently from each other choose respectively the personal (private) keys l_A and l_B such that $1 < l_A, l_B < 2^m$.

4. Then users *A* and *B* calculate the third element of the public key respectively:

$$\beta_A(x) = (\beta_{A_1}(x), \beta_{A_2}(x),..., \beta_{A_S}(x))\text{, where}$$

$$\beta_{A_i}(x) \equiv \alpha_i^{l_A}(x)(\mathrm{mod}(p_i(x)),\ i = \overline{1,S}\ ;$$

$$\beta_B(x) = (\beta_{B_1}(x), \beta_{B_2}(x),..., \beta_{B_S}(x))\text{, where}$$

$$\beta_{B_i}(x) \equiv \alpha_i^{l_B}(x)(\mathrm{mod}(p_i(x)),\ i = \overline{1,S}.$$

All operations of exponentiation are performed in non-positional polynomial notation, so the calculation of these operations can be performed in parallel modulo the polynomials chosen as base numbers of NPNs.

5. Then parties *A* and *B* exchange the calculated values of the public keys

$$K_A(x) = (P_S(x), \alpha(x), \beta_A(x)),\ K_B(x) = (P_S(x), \alpha(x), \beta_B(x))$$

respectively by the unprotected channel in binary representation. The users fix in advance the values of working

bases $p_1(x), p_2(x),..., p_S(x)$ and of generating elements $\alpha_1(x), \alpha_2(x),..., \alpha_S(x)$, and their order of the arrangement. In this regard, by the unprotected channel only the general form $P_S(x), \alpha(x)$ and $\beta(x)$ is transferred in binary representation.

6. Using public keys of the addressee, users *A* and *B* carry out the process of encryption E_k of the message *M* by analogy with the traditional ElGamal scheme:

$$E_k(M) = (C_1, C_2),\ C_1 = \alpha^r (\mathrm{mod}(P_S(x)),$$
$$C_2 = M \cdot \beta^r (\mathrm{mod}(P_S(x)),$$

where r - incidentally chosen number (randomizer) and $0 \le r \le 2^m$. We should note that it is possible to choose different randomizers for each base number of NPNs.

7. For decrypting D_k of the encrypted message, the users *A* and *B* apply their personal keys according to the formula:

$$D_k(C_1, C_2) = C_2 \cdot (C_1^{l_i})^{-1} \bmod P_S(x) = M,$$

where $i = A, B$.

All calculations in NPNs can be made in parallel modulo base numbers $p_1(x), p_2(x),..., p_S(x)$, thereof the essential increase of the performance speed of operations is possible.

Reliability of the offered algorithm increases owing to the choice of the base numbers of NPNs and the corresponding generating elements. Another advantage is the possibility of reduction of performance time of arithmetic operations owing to their parallelization modulo the base numbers of NPNs.

III. Modeling of Software Realization of Asymmetric Non-Positional System of Encryption

For the purpose of studying and analyzing the advantages of the modified ElGamal cryptosystem algorithm of encryption, its software realization in language C ++ has been made. The program windows are given in figures 1 and 2. The computer program consists of two interconnected blocks (subprogrammes): the system of formation of private and public keys, the system of encryption. These subprogrammes are started for the performance by buttons of the Key and Crypto tabs respectively.

In the block of formation of private and public keys the following procedures are realized:
- calculation of irreducible polynomials of the set degree with binary coefficients and selection of working base numbers;
- finding of primitive polynomials over the chosen working base numbers;
- calculation of public and private keys.

In the block of encryption of electronic messages the main modules are:
- choice of public key of the recipient;
- choice of a random number (randomizer);
- encryption of a message and decryption of a cryptogram.

In the course of the computer realization of the modified algorithm of encryption according to the El-Gamal scheme, a possibility of acceleration of calculations while performing an operation of exponentiation modulo the working base numbers of NPNs has been revealed

When forming the encryption keys, irreducible polynomials of the set degree over the field GF(2) and the primitive elements (polynomials) corresponding to them have been defined. The calculated irreducible polynomials are preserved in the database of keys. They are used when forming public and private keys. Public keys of other users are accepted as a file, which will also be stored in the database of keys. In the process of the performance, the subprogramme "Key" generates, exports and imports the encryption keys. (figure 1).

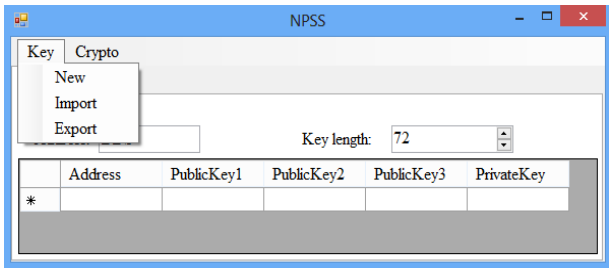

Figure 1 - The Key tab. window

The user of the program creates the key couple: public and private key. While generating the keys, their owner, the key length and the term of its action are set. The public key is used for encryption of the initial message, and the private key — for decryption of the cryptogram.

The length of the key is defined by the user. The period of the key validity can be defined as unlimited or till the concrete date. For the key protection, the program will be upgraded, it is planned to use hashing with the application of the confidential phrase. The exported keys are stored and transferred as a file.

The subprogramme "Crypto" realizes the encryption system and preserves the encrypted files and decrypted cryptotexts (figure 2).

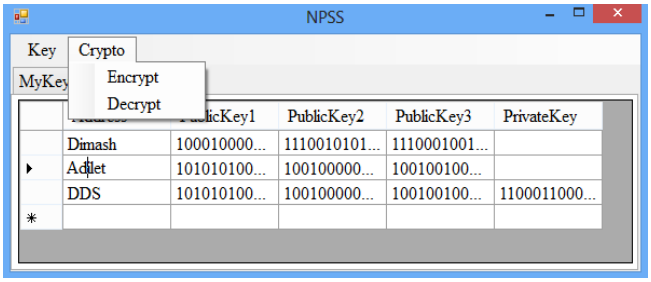

Figure 2 - The Crypto tab. Window

In the process of NPNs creation it is planned to carry out the choice of the working base numbers in two ways. In the first case the working base numbers will be chosen out of the developed database of irreducible polynomials, and in the second case they will be generated in the course of the

performance of the cryptoalgorithm on the set interval of values of the degree of irreducible polynomials.

Throughout the presented results on the development and realization of the modified encryption system, the creation of the certification center is planned. The warrant of the certificate will mean that the key really belongs to the specified owner and can be used for the signature of certificates of one level lower. Also it will specify the way of the cancellation of the certificate. It is necessary for ensuring safety in case of loss or compromise of the private key.

The problem of the correct definition of belonging of public key to the owner is characteristic for all cryptographic systems with asymmetric encryption. It has no enough good solutions. The proposed solutions (similar to the PGP scheme) allow the user to solve whether to use the scheme of the verification of certificates.

IV. Conclusion

For the Republic of Kazakhstan the development of cryptographic means of ensuring the information security is an actual task. Scientific researches on this subject are devoted to the development and software realization of asymmetric non-positional systems of encryption. The modified asymmetric system of encryption on the basis of non-positional polynomial notations (NPNs) with use of the algorithm of encryption according to the El-Gamal scheme has been developed.

For the purpose of the analysis of non-positional El-Gamal encryption algorithm, the model of its software realization has been constructed. The realized model consists of two interconnected blocks: the formation of private and public keys, the system of encryption and decryption. Work of the computer program is verified on concrete examples. On the basis of this program the features of the asymmetric El-Gamal encryption system modified on the NPNs basis will be investigated.

References

[1] W. Diffie, M. Hellman, “Privacy and Authentication: An Introduction to Cryptography,” Proc. of the IEEE [Russian Translation]. No.3, 1979, pp.71–109.

[2] T. El Gamal, “A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, IEEE Transactions on Information Theory, v. IT-31, n. 4, 1985. pp. 469-472.

[3] Menezes A., Orschot P. and Vanstone S. Handbook of Applied Cryptography - CRC Press, 1996.

[4] W. Stallings, “Cryptography and Network Security (4th Edition),” Prentice Hall, 2005.

[5] Shahzadi Farah, M. Younas Javed, Azra Shamim, Tabassam Nawaz. An Experimental Study on Performance Evaluation of Asymmetric Encryption Algorithms // Proceedings of the 3rd European Conference of Computer Science (ECCS '12). - Paris, France 121-124 pp., 2012.

[6] Laura Savu. Cryptography Role in Information Security // Recent Researches in Communications and IT (CITCOM-04). - Corfu Island, Greece, 36-41 pp., 2011.

[7] I. Ya. Akushskii, D. I. Juditskii, “Machine Arithmetic in Residue Classes [in Russian],” Moscow: Sov. Radio, 1968.

[8] R. G. Biyashev, “Development and investigation of methods of the overall increase in reliability in data exchange systems of distributed ACSs,” Doctoral Dissertation in Technical Sciences, Moscow, 1985.

[9] R. G. Bijashev, S. E. Nyssanbayeva Algorithm for Creation a Digital Signature with Error Detection and Correction // Cybernetics and Systems Analysis. – 2012. – Vol. 48, No 4, pp. 489-497.

[10] Biyashev R.G., Nyssanbayeva S.E., Begimbayeva Ye.Ye., Magzom M.M. Modification of the cryptographic algorithms, developed on the basis of nonpositional polynomial notations // Proceedings of the International Conference on Circuits, Systems, Signal Processing, Communications and Computers (CSSCC 2015), - Vienna, Austria., 170-176 pp., 2015.