Academic Research in Educational Sciences VOLUME 2 | ISSUE 10 | 2021
ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
Directory Indexing of International Research Journals-CiteFactor 2020-21: 0.89
DOI: 10.24412/2181-1385-2021-10-89-93

INVESTIGATION OF THE POSSIBILITY OF USING MATRIX MULTIPLICATION IN ASYMMETRIC CRYPTOGRAPHIC SYSTEMS

Alisher Mavlonov
National University of Uzbekistan named after Mirzo Ulugbek

ABSTRACT

The paper considers aspects of the use of matrix multiplication in asymmetric cryptographic systems. The possibilities of using matrix multiplication in a finite field are shown when creating asymmetric cryptosystems.

Keywords: asymmetric cryptographic systems, cryptographic strength, matrix, matrix multiplication in a finite field.

INTRODUCTION

At present, symmetric and asymmetric cryptographic systems are widely used to ensure the confidentiality of information. Symmetric encryption algorithms can be considered sufficiently studied and effective; these types of ciphers have a high encryption speed. The main disadvantage of symmetric encryption is the need for public hand-to-hand transmission of encryption keys. One cannot but pay attention to this drawback, since with such a system it becomes almost impossible to use symmetric encryption with an unlimited number of participants. However, this disadvantage of symmetric ciphers can be overcome by using asymmetric cryptographic systems to transmit the encryption key. Asymmetric cryptosystems are also used successfully in electronic digital signature applications.

Often, the strength of symmetric block cipher algorithms, especially to differential and linear cryptanalysis, depends on the choice of values in substitution tables (S-boxes) [1,2]. Mathematically, the cryptographic strength of asymmetric encryption algorithms has not yet been proven. The cryptographic strength of asymmetric cryptosystems is based mainly on the algorithmic difficulty of solving a problem in a reasonable time.

It should be borne in mind that today the problems of asymmetric cryptography have become a self-sufficient area of research. The issues of building cryptographic protocols, zero-knowledge proofs, number-theoretic aspects of asymmetric cryptography are constantly among the discussed problems.

MATERIALS AND METHODS

Practically used algorithms of asymmetric cryptography are based on two problems [3]: discrete logarithm and factorization. There are different opinions about the possibility of solving these problems in the future, and how soon this may happen. Therefore, for specialists in the field of information security, the task of developing alternative systems remains relevant. In this case, the main problems remain the existence of a one-way function and a function with a secret. The following areas of research should be highlighted here:

1. The global theoretical idea of constructing new asymmetric cryptosystems is to try to generate functions with a secret by "masking" simple problems for complex (NP-complete) ones. Many options were proposed, but they all proved to be unstable.

2. The results obtained on opening some variants of the cryptoscheme on the basis of the "knapsack" problem have formed a skeptical attitude towards all such schemes in the environment of cryptographers-practitioners. At the same time, formally, the Shore-Rivest scheme has not been cracked to this day. A number of theoretical cryptographers consider the "knapsack" problem to be one of the most promising for constructing asymmetric cryptography algorithms, since "complexity" is inherent in its very nature.

3. The scheme of public key distribution using non-commutative groups was proposed by the laboratory of Moscow State University for mathematical problems of cryptography in 1993, which was a fundamentally new approach to this problem. However, to date, no practically realizable schemes based on these ideas have been proposed.

4. After Sidelnikov and Shestakov, using fast decoding algorithms, showed that one of the Mac-Eliece type schemes (Niederreiter's scheme) is unstable, a number of variants of the scheme based on code-theoretic constructions were proposed. None of them has found practical application either because of its cumbersomeness, or because its durability raises great doubts among specialists.

5. Since the beginning of the 90s, the possibility of implementing asymmetric cryptography protocols based on quantum mechanical effects has been widely discussed.

As shown by a comparative analysis of existing asymmetric cryptosystems, one of the significant disadvantages of encryption is the low encryption speed in their software and/or hardware-software implementation in comparison with symmetric encryption algorithms (hundreds, and sometimes thousands of times slower than symmetric encryption algorithms). For this reason, asymmetric algorithms are now used mainly to encrypt low-volume information.

Research in this direction is aimed at developing a new high-speed asymmetric encryption algorithm and software for it [4].

Based on this goal, the following tasks follow:

1. Classification and analysis of existing asymmetric cryptosystems;
2. Study of matrices with a special structure as a one-way function;
3. Development of asymmetric cryptosystems based on matrices with a special structure;
4. Evaluation of the effectiveness of the developed asymmetric cryptosystems based on matrices with a special structure;
5. Development of a library of realizing asymmetric cryptosystems based on matrices with a special structure;

RESULTS AND DISCUSSION

Let a A_{mxn} matrix be given in a finite field G (N), if $m \geq n$, then for the A_{mxn} matrix there exists a B_{nxm} matrix such that multiplication by E_{nxn} which is equal to the identity matrix in a finite field G (N) [5].

$$B_{nxm} A_{mxn} (\bmod N) = E_{nxn} (\bmod N)$$

or

$$\begin{pmatrix} b_{11} & b_{12} & \dots & b_{1m} \\ b_{21} & b_{22} & \dots & b_{2m} \\ \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{nm} \end{pmatrix} * \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} (\bmod N) = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} (\bmod N)$$

In order to calculate the inverse of a A_{mxn} matrix in a finite field, the following steps are performed:

1. The K_{nxm} matrix in the finite field G (N) is arbitrarily chosen K_{nxm} and the A_{mxn} matrix multiplied and the F_{nxn} matrix is calculated.

$$F_{nxn} = K_{nxm} * A_{mxn} (\bmod N)$$

$$F_{nxn} = \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \dots & \dots & \dots & \dots \\ k_{n1} & k_{n2} & \dots & k_{nm} \end{pmatrix} * \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} (\bmod N) = \begin{pmatrix} f_{11} & f_{12} & \dots & f_{1n} \\ f_{21} & f_{22} & \dots & f_{2n} \\ \dots & \dots & \dots & \dots \\ f_{n1} & f_{n2} & \dots & f_{nn} \end{pmatrix} (\bmod N)$$

2. The determinant of the F_{nxn} matrix is calculated.

ISSN: 2181-1385
Scientific Journal Impact Factor (SJIF) 2021: 5.723
Directory Indexing of International Research Journals-CiteFactor 2020-21: 0.89
DOI: 10.24412/2181-1385-2021-10-89-93

$$\Delta = |F_{nxn}| = \sum_{i=1}^{n} (-1)^{i+l} f_{il} A_{il} (\bmod N),$$

here $l = const$ $(1 \le l \ge n)$, A_{il} - algebraic complements. If, $GCD(\Delta, N) \ne 1$ then 1-stage is executed again.

3. Calculate the multiplicative inverse of the Δ determinant modulo *N*.

$$D = \Delta^{-1} (\bmod N) \text{ or } \Delta * D = 1 (\bmod N)$$

4. The value D is multiplied by the transposed matrix S_{nxn}, obtained by the algebraic complements of the F_{nxn} matrix. The result is a T_{nxn} matrix inverse to the F_{nxn} matrix modulo *N*.

$$T_{nxn} = \Delta * (S_{nxn})' (\bmod N)$$

$$T_{nxn} = \Delta * \begin{pmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \dots & \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{pmatrix} (\bmod N) = \begin{pmatrix} \Delta A_{11} & \Delta A_{12} & \dots & \Delta A_{1n} \\ \Delta A_{21} & \Delta A_{22} & \dots & \Delta A_{2n} \\ \dots & \dots & \dots & \dots \\ \Delta A_{n1} & \Delta A_{n2} & \dots & \Delta A_{nn} \end{pmatrix} (\bmod N)$$

5. By multiplying a T_{nxn} matrix by a K_{nxm} matrix modulo N, the B_{nxm} matrix is calculated.

$$B_{nxm} = T_{nxn} * K_{nxm} (\bmod N)$$

This construct can be used when encrypting data. If we accept the A_{mxn} matrix as the public key, and the B_{nxm} matrix as the private key, then the encryption and decryption process can be carried out according to the following rules:

Encryption: $Y_{mx1} = A_{mxn} * X_{nx1} (\bmod N)$

Decryption: $X_{nx1} = B_{nxm} * Y_{mx1} (\bmod N)$

Here, X_{nx1} - is the vector representation of the plaintext block, Y_{mx1} - is the vector representation of the cipher text block.

CONCLUSION

Indeed, given the equality, $B_{nxm} A_{mxn} (\bmod N) = E_{nxn} (\bmod N)$ the following holds:

$$X_{nx1} = B_{nxm} * Y_{mx1} (\bmod N) = B_{nxm} * A_{mxn} * X_{nx1} (\bmod N) = E_{nxn} * X_{nx1} (\bmod N) = X_{nx1}$$

The above construction cannot be used as an asymmetric encryption algorithm in the same form, since the A_{mxn} public key being known makes it possible to find the B_{nxm} private key. An attacker can easily find the private key B_{nxm} by following the above steps. We are still researching ways to solve the problem in the master, and the following articles will discuss this work.

REFERENCES

1. Timur Abdullaev and Gayrat Juraev. Development of a Method for Generating Substitution Tables for Binary and Ternary Number Systems. AIP Publishing: AIP Conference Proceedings “International Uzbekistan-Malaysia Conference on “Computational models and technologies (CMT2020)”, Volume 2365. Melville, New York, 2021.P. 040003-1 – 040003-11.
2. Timur Abdullaev and Gayrat Juraev. Selection of the Optimal Type of the Gamming Function for Symmetric Encryption Algorithms. AIP Publishing: AIP Conference Proceedings “International Uzbekistan-Malaysia Conference on “Computational models and technologies (CMT2020)”, Volume 2365. Melville, New York, 2021, P. 040004-1 – 040003-13.
3. Moldovyan N.A., Moldovyan A.A., Introduction to public key cryptosystems – Sankt - Peterburg, BHV-Peterburg, 2005.
4. Jumaniyazov M.O. On the relevance of the development of asymmetric data encryption algorithms. Republican seminar: “Information security in the field of communications, informatization and telecommunication technologies. Problems and ways to solve them. Collection of abstracts and reports. Tashkent October 29, 2013. P.101-103. (In Russian)
5. Gantmacher F.R. The Theory of Matrices. Nauka, Moscow, (1967) (In Russian)