УДК 514.18

USING OF CURVES AND SURFACES IN CRYPTOGRAPHY

A. Lebedko, V. Urchenko, V. Kycherenko, A. Naydish

In the article describes the use of curves and surfaces defined in BN-calculus in the solution of problems of a cryptographic nature.

Keywords: elliptic curve crypto, cryptography, surface-point calculus Balyuby Naydysha.

Formulation of the problem. The problem of data protection from hacking becomes more acute every year. This is due to the emergence of new algorithms of cryptanalysis and the increase in the computing power of modern computers, which makes it possible to successfully use even simple search algorithms for objects that have a low level of protection. And although most data hacking cases are associated with "holes" in security systems, and not with cracking the cipher itself or by selecting a password, it is simply impossible to ignore the modernization of data encryption, especially since in the modern world the process of hacking and stealing data has become a highly profitable Business, and the number of hacker attacks is growing with an avalanche rate.

Analysis of recent research and publications. In [1,2], as well as in the works of many other authors, the application of elliptic curves on finite fields is described for data encryption. A brief analysis of the advantages and disadvantages of this method of encryption was carried out in [3]. The general advantages of methods based on elliptical curves, in comparison with cryptographic algorithms with a public key, based on the problem of factorization of large numbers (RSA) and discrete logarithms (El-Gamal) and widely used in practice, boil down to obtaining the same level of cryptographic strength with more Short key length. Problems with the use of elliptical algorithms boil down to purely technical aspects, which include the refusal of some organizations to switch to new encryption protocols, and also to certify elliptical cryptography.

In work [4], as well as other works of these authors, it is proposed to modernize elliptic encryption by applying Edwards curves, as well as curves in the Weierstrass form.

Formulation of the purpose of the article. Conduct an analysis of the possibilities of obtaining new methods of data encryption based on geometric algorithms using point BN-calculus.

Main part. As noted in many modern sources, with every new leap of mankind in the field of the development of computer technology and, as

a result, the increase in computing power, the possibilities in using all new mathematical algorithms for hacking and stealing protected data are growing.

Over the last decade, algorithms for encrypting data based on elliptical curves are actively developing and being introduced into protective systems. This method is not devoid of shortcomings, but, nevertheless, it is a good alternative to the algorithms currently used in the vast majority of computer systems.

The basis of the encryption algorithm based on the elliptic curve is a one-parameter relationship - the point that belongs to the curve. Consider a general encryption algorithm for an individual block [5]:

1. The decimal value of the block (letters) *t*.
2. A random number is selected *k* (*0*<*k*<*n*).
3. The point $P_k(x_{Pk}, y_{Pk}) = k * P$.
4. The point $Q_k(x_{Qk}, y_{Qk}) = k * Q$.
5. Calculated $c = (t * x_{Pk}) \bmod n$.
6. Get the cipher message - pair [P_k, c].

Thus, encryption based on an elliptical curve is a variation of El-Gamal's encryption. If the stability of the algorithm of El-Gamal encryption is based on the complexity of solving the discrete logarithm problem, then the stability of encryption using elliptic curves is based on the complexity of finding the factor k of the point P by their product. Those, if $Q = k * P$, Then knowing P and k is fairly easy to compute Q. An effective solution to the inverse problem-to find k for known P and Q, has not yet been published.

The essence of the forthcoming work consists in the modernization of the elliptic method of encryption using point BN-calculus [3] and the proposal of new methods based on the use of geometric algorithms.

It is known that any curve, including elliptic curves, is a one-parameter set of points. Any surface, in turn, is a one-parameter set of straight or curved lines. Thus, the surface can be considered as a two-parameter set of points or as a multiparameter for surfaces in spaces with dimension greater than 3.

This feature of the surface, in our opinion, is appropriate to use to encrypt the "login / password" pair (by the number of operating parameters). In aggregate, the presence of two parameters having a finite length, as well as the existence of a huge number of all possible surfaces, in the presence of even an average complex encryption algorithm, will provide a sufficiently high cryptographic strength of this method of information protection.

In the theory of the apparatus of point BN-calculus, at the moment, a significant amount of the geometric representation of surfaces with various pre-set properties has been developed, but, in our opinion, the most appropriate is the use of the "Loop" method presented in [6]. This method is noteworthy in that the surface is divided into rectilinear segments with a uniform or uneven pitch, or curved segments with an uneven pitch that varies within one of the guides. At the same time, the number of cells that will be part of the segment on which the magnifying glass is directed will depend on the order of the curves that limit this segment. The reference points for the method will be the numerical values of the encrypted pair "login / password".

Conclusions. The article considers encryption aspects on the basis of an elliptical curve from the point of view of applied geometry and suggests a way to increase the cryptographic stability of data by using the plane as the base object for encryption, which will improve the reliability of information.

Literature

1. Эксперты призывают готовиться к криптоапокалипсису [Електронний ресурс]. – Режим доступу: URL: http://habrahabr.ru/ post/188846/.
2. Элементарное введение в эллиптическую криптографию / А.А. Болотов, С.Б. Гашков, А.Б. Фролов, А.А. Часовских. – М.: КомКнига, 2006. – 608 с.
3. Лебідько О.С. Використання скручених кривих едвардса у криптографії / О. С. Лебідько, В. О. Лебедєв // Збірник тез доповідей XI Міжнародної науково-практичної конференції «Обухівські читання» (1-го березня 2016 року) / Національний університет біоресурсів і природокористування України. – К., 2016. – 24-25 с.
4. Бессалов А.В. Сравнительная оценка быстродействия канонических эллиптических кривых и кривых в форме Эдвардса над конечным полем / А.В. Бессалов, А.А. Дихтенко, Д.Б. Третьяков // Сучасний захист інформації. – №4. – 2011. – С. 33–36.
5. Криптографические методы защиты информации [Електронний ресурс]. – Режим доступу: URL: https://sites.google.com/site/ anisimovkhv/learning/kripto/lecture/tema8.
6. Кучеренко В. В. Формалізовані геометричні моделі нерегулярної поверхні для гіперкількісної дискретної скінченої множини точок : дис... канд. техн. наук: 05.01.01 / В. В. Кучеренко . – Мелітополь: ТДАТУ, 2013. – 208 с.