

**A MODIFIED METHOD OF ENCRYPTING TEST DATA  
WITH ELLIPTIC CURVES USING A UNIQUE ALPHABETIC KEY STRING**

*P. SINITSA, D. PASTUKHOV*  
Polotsk State University, Belarus

*In the paper presents the mathematics of elliptic curves. As well as the derivation of addition formulas and doubling elliptic points. A description of the encryption and decryption algorithm is presented. The work of the developed program based on the mathematics of elliptic curves in the console is shown.*

**Introduction.** Elliptic cryptography is a section of cryptography that studies asymmetric cryptosystems based on elliptic curves over finite fields. The main advantage of elliptic cryptography is that today, the existence of subexponential algorithms for solving the discrete logarithm problem is unknown. The role of the main cryptographic operation is performed by the operation of scalar multiplication of a point on an elliptic curve by a given integer, determined through the addition and doubling of the points of the elliptic curve. The latter, in turn, are performed on the basis of the addition, multiplication and inversion operations in the final field, over which the curve is considered. Of particular interest in the cryptography of elliptic curves is due to the advantages that its use in wireless communications provides - high speed and short key length.

**The mathematics of elliptic curves.** Cryptographic methods use elliptic curves over a field of integers with a field characteristic  $r = 2$  or more  $r \geq 3$ . In the future, we will consider the field of integers with the characteristic  $r \geq 3$ .

Cryptographic curves with characteristic  $r > 3$  have the canonical form:

$$y^2 = x^3 + ax + b \quad (1)$$

Where  $a, b$  are integer coefficients of the curve,  $p$  is a simple sufficiently large number. As can be seen from formula (1), if the point with coordinates  $(x, y)$  satisfies equation (1), then point  $c(x, -y)$  also satisfies equation (1). An elliptic curve is understood to mean a geometric set of points (1) supplemented by an infinitely remote point.

The following number is called the discriminant of the curve:  $\Delta = -16(4a^3 + 27b^2)$ , the discriminant must not be zero (in this case, there are no self-intersection points and return points). If the discriminant is positive  $\Delta > 0$ , then the graph has 2 parts, if  $\Delta < 0$ , then one part.

On the set of points of an elliptic curve, a group is determined by the addition of points of the elliptic curve (the section of mathematics is called algebraic geometry). The sum of two points of the elliptic curve  $P, Q$  is the third point  $R$  lying on the line  $PQ$  and the elliptic curve at the same time, and is denoted as  $R = P + Q$ , i.e.  $-R + P + Q = 0$ . The operation of group addition is called 3 points of an elliptic curve that satisfy the equation:

$$R' + P + Q = 0. \quad (2)$$

This shows that  $R' = -R$  ( $R', R$  are elements mutually inverse in the group operation). On the other hand, a straight line parallel to the coordinate axis  $y$  intersects exactly 2 points of elliptic curves (mirror symmetric about the  $x$  axis) and an infinitely distant point (in opposite directions), therefore, the mutually inverse points of the elliptic curves  $R', R$  have coordinates  $(x, y)$  and  $(x, -y)$ , respectively. A group addition group defines a geometrically infinitely distant point and denotes  $0$ . So, for a group addition operation, it is necessary to draw a secant through the points  $P, Q$  and mirror the point  $R, R' = -R$ .

Special cases are possible:

- 1)  $P = Q$  - the secant line degenerates into the tangent  $R' + 2P = 0$
- 2)  $P + Q + 0 = 0 \Leftrightarrow P = -Q$  points  $P, Q$  (mirror symmetric) have the same abscissas. The next point in addition is the point  $Q + 0 = Q$  (the forming element of the abelian group).
- 3)  $P + P + 0 = 0 \Leftrightarrow P = 0$  - the secant line is simultaneously a vertical line and a tangent. Cryptography uses finite cyclic abelian groups with a generating element  $G$ . Moreover, any point of the elliptic curve of the cyclic group  $1 \leq k \leq n_0$  is obtained by the formula:  $P_k = (GG \dots G)$ . The order of the group of points of an elliptic curve is the number  $n_0$  such that  $P_{n_0} = 0$  is the zero element of the group. Knowing the generating element of the group  $G$ , we can compile a table of all points of the elliptic curve, when adding points with order  $k > n_0$ ,

all points are periodically repeated:  $P_k = P_{k-n_0-s}$ , where  $1 \leq k - n_0 + s \leq n_0 - 1$ ,  $s \in \mathbb{N}$ . Depending on the general situation of particular cases 1), 2), 3) the coordinates of the points of the elliptic curve are calculated by the formulas (indices 1 and 2 correspond to points P, Q, respectively):

$$\begin{cases} x = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 = k^2 - x_1 - x_2 \\ y = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x) = -y_1 + k(2x_1 - x_2 - k^2) \end{cases} \quad (3)$$

$$\begin{cases} x = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 = k^2 - 2x_1 \\ y = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x) = -y_1 + k(3x_1 - k^2) \end{cases} \quad (4)$$

The derivation of formulas (3) and (4):

The angular coefficient of a straight line passing through 2 points is:  $k = \frac{y_2 - y_1}{x_2 - x_1} = \frac{y - y_1}{x - x_1}$ , where the

point of the line  $(x, y)$  is moving along the line. We get for points 1 $(x_1, y_1)$ , 2 $(x_2, y_2)$ ,  $(x, y)$ :

$$\begin{aligned} y^2 &= x^2 + ax + b, \\ y_1^2 &= x_1^2 + ax + b, \\ y_2^2 &= x_2^2 + ax + b. \end{aligned}$$

Subtract  $(y_2 - y_1)(y_2 + y_1) = (x_2 - x_1)(x_2^2 + x_1x_2 + x_1^2) + a(x_2 - x_1)$ , where

$$k = \frac{y_2 - y_1}{x_2 - x_1}, k(y_2 + y_1) = (x_2^2 + x_1x_2 + x_1^2) + a, \text{ similarly,}$$

$$k = \frac{y - y_1}{x - x_1}, k(y + y_1) = (x^2 + x_1x + x_1^2) + a, \text{ and the last formula}$$

$$k = \frac{y - y_2}{x - x_2}, k(y + y_2) = (x^2 + x_2x + x_2^2) + a.$$

Subtract the second from the third formula, we get  $k(y_2 - y_1) = x(x_2 - x_1) + (x_2 - x_1)(x_2 + x_1)$

Where  $k^2 = x + x_2 + x_1 \Leftrightarrow x = k^2 - x_2 - x_1$ .

For coordinate  $y = y_1 + k(x - x_1) = y_1 + k(k^2 - 2x_1 - x_2)$ . It remains to recall that for a group operation you need to select a mirror point :

$$(x, -y) = (k^2 - x_2 - x_1, -y_1 + k(-k^2 + 2x_1 + x_2)) \quad (5)$$

Thus, formula (3) is proved.

If the secant is tangent, we get  $x_2 = x_1, x = k^2 - 2x_1$

Next, we differentiate equation 1) with respect to x:

$$2yy' = 3x^2 + a, \Leftrightarrow k = y' = \frac{3x^2 + a}{2y} = \frac{3x_1^2 + a}{2y_1},$$

From formula (5) we obtain  $(x, -y) = (k^2 - 2x_1, -y_1 + k(-k^2 + 3x_1)), k = \frac{3x_1 + a}{2y_1}$ . Thus, formula (4) is

proved. The cyclic group is formed from the set of points of the elliptic curve (equation (1)), connected by a geometric group structure (formulas (3), (4)), supplemented by a field integer structure in

Modulus of a prime p, i.e. instead of (1) solve comparisons:

$$y^2 = x^3 + ax + b \pmod{p} \tag{6}$$

Ultimately, we use formulas (3), (4) and (6), obtaining successively all points of the elliptic curve of a cyclic abelian group. As can be seen from formulas 3) and 4), the coordinates of the points of the elliptic curve are rational numbers if the first 2 points of the curve are also rational, i.e. geometric group operation leaves the coordinates of the points rational further. An analysis of formulas (3) and (4) shows that if the angular coefficient of the line takes integer values, then the x, y coordinates will continue to be integer. Thus, it is necessary to solve the comparison:

$$\begin{cases} \frac{y_2 - y_1}{x_2 - x_1} \equiv (y_2 - y_1) \pmod{p} * (x_2 - x_1)^{-1} \pmod{p}, (x_2 - x_1)(x_2 - x_1)^{-1} \equiv 1 \pmod{p} \\ \frac{3x_1^2 + a}{2y_1} \equiv (3x_1^2 + a) \pmod{p} * (2y_1)^{-1} \pmod{p}, (2y_1) * (2y_1)^{-1} \equiv 1 \pmod{p} \end{cases} \tag{7}$$

A brief description of the algorithm for constructing a sequence of points:

- 1) Find the inverse element in (7) to  $2y_1$ , or to  $x_2 - x_1$ .
- 2) Find the numbers  $k_1 = (y_2 - y_1) \pmod{p} * (x_2 - x_1)^{-1} \pmod{p}$ , or  $k_1 = (3x_1^2 + a) \pmod{p} * (2y_1)^{-1} \pmod{p}$ .
- 3) Find the numbers

$$\begin{cases} x = (k_1^2 - x_1 - x_2) \pmod{p} \\ y = (-y_1 + k_1(2x_1 + x_2 - k_1^2)) \pmod{p} \end{cases} \tag{8}$$

Either by the formulas:

$$\begin{cases} x = (k_1^2 - 2x_1) \pmod{p} \\ y = (-y_1 + k_1(3x_1 - k_1^2)) \pmod{p} \end{cases} \tag{9}$$

**Description of the encryption and decryption algorithm**

The encryption and decryption formula is as follows:

$(kG, P_m + k * P_b)$  (encryption) - -  $\rightarrow P_m + k * n_b * G - n_b * k * G = P_m$  (decryption), where  $n_b$  is the private key of subscriber b and  $P_b$  is the public key of subscriber b.

The message (number) should be equal to the difference of the x coordinate and the coordinate of the points of the elliptic curve. Since this is not possible for all residues modulo a prime number p. Then we create our own alphabetical string, which is also an additional encryption key, in which there are all letters of the Latin alphabet and all numbers arranged in order as in the English alphabet or not in order. In addition, you have to make spaces to fill them with an asterisk. The idea is as follows. It is necessary to arrange all the letters and numbers in the alphabetical line at those positions (serial numbers) for which there is an elliptic curve point whose coordinate difference is equal to the position number of the letter in the alphabetical line. Thus, we display the numbers of all letters in the alphabetical string at the points of the elliptic curve. An example of an alphabetical string: '\* b \* a \*\*\* cdefghi \* jkl \*\* mnopqrs \*\* tuvxyz01 \* 2 \*\* 3456789 \*\*'.

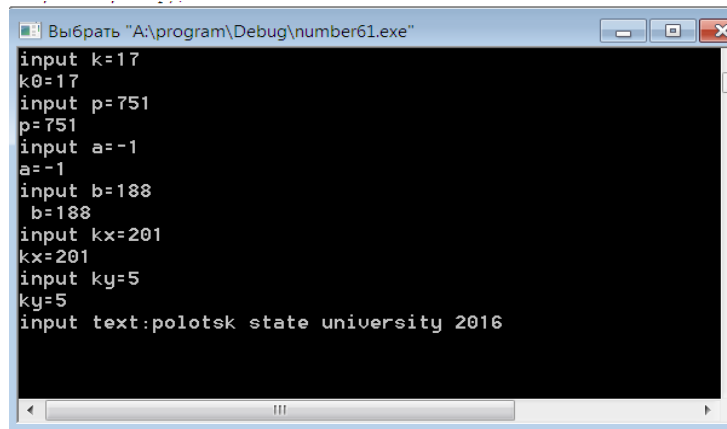
Further, letters are read out from another line-word by characters and written into its array. After, the next character of the word and the characters of the alphabetical string are compared. As soon as the letters coincide, the word symbol is mapped to the position number in the alphabetical location line of this symbol and its corresponding elliptic curve point, the difference of coordinates of which is equal to the given position of the symbol in the alphabetical line. When deciphering by the found point, you need to subtract its x and y coordinates and read the symbol with the given position in the alphabetical string and write this letter of the alphabet at the output. Alphabetical strings are determined experimentally, so that all letters and punctuation marks, numbers of the English alphabet are encrypted and decrypted uniquely using elliptical cryptography.

**Testing the program in the console.** We enter a phrase to test data encryption: "polotsk state university 2019" with a string length of  $nn = 29$ . The result of text entry, the parameters of the elliptic curve  $a = -1, b = 188, p = 751$ , the public key  $(k_x, k_y) = (201, 5)$  are shown in Figure 1.

We see the result of encryption and decryption in Figure 2. Each source character of the text corresponds to four integer coordinates of two points of the elliptic curve located on one line. For ease of input and line-

by-line reading, the same cipher in one column is written to the text file balka1.txt. We see a complete coincidence of the cipher in two stages.

In addition, it is also seen that the random number  $k = 17$  introduced into the program in Figure 1 and recorded by the program in the text file balka2.txt also match.

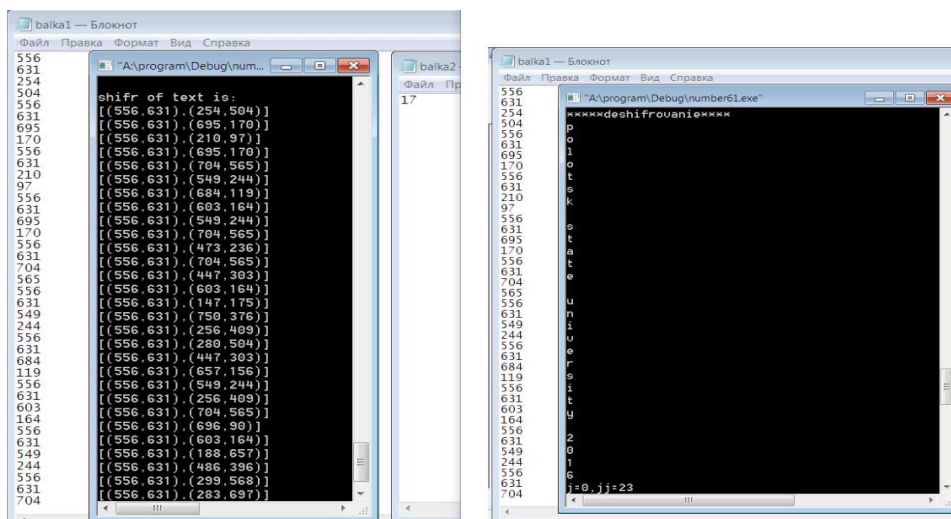


```

input k=17
k0=17
input p=751
p=751
input a=-1
a=-1
input b=188
b=188
input kx=201
kx=201
input ky=5
ky=5
input text:polotsk state university 2016
  
```

Figure 1. – Entering data into the program

The encryption protocol indicates the coordinates of the point of the elliptic curve corresponding to each input character and the difference of the coordinates of the x-y point, which is equal to the position of the original character in the alphabetical string. For example, from a point of an elliptic curve with coordinates  $(x_m, y_m) = (680, 657)$ ,  $des = x_m - y_m = 680 - 657 = 23$  the original character using the alphabetical string (the numbering of characters in the alphabetical string starts from zero, therefore  $des = 23$  matches 24 characters, i.e. Latin letter p (Fig. 2 below).



```

shifr of text is:
[(556,631),(254,504)]
[(556,631),(695,170)]
[(556,631),(210,97)]
[(556,631),(695,170)]
[(556,631),(704,565)]
[(556,631),(549,244)]
[(556,631),(684,119)]
[(556,631),(603,164)]
[(556,631),(549,244)]
[(556,631),(704,565)]
[(556,631),(473,236)]
[(556,631),(704,565)]
[(556,631),(447,303)]
[(556,631),(603,164)]
[(556,631),(147,175)]
[(556,631),(750,376)]
[(556,631),(256,409)]
[(556,631),(289,594)]
[(556,631),(447,303)]
[(556,631),(657,156)]
[(556,631),(549,244)]
[(556,631),(256,409)]
[(556,631),(704,565)]
[(556,631),(696,90)]
[(556,631),(603,164)]
[(556,631),(188,657)]
[(556,631),(486,396)]
[(556,631),(299,568)]
[(556,631),(283,697)]
  
```

```

*****deshifrovani*****
p
o
l
o
t
s
k
s
t
a
t
e
u
n
i
v
e
r
s
i
t
y
2
0
1
6
j=0, jj=23
  
```

Figure 2. – The result of the operation of encryption (left) and decryption (right)

Indeed, the phrase “polotsk state university 2019” begins with the letter p. Second character  $(x_m, y_m) = (266, 244)$ ,  $des = x_m - y_m = 266 - 244 = 22$  matches 23 in a row character in the alphabetical string, i.e. latin letter o, which corresponds to the second letter in the word polotsk. It can be seen from the console that the cipher has other coordinates than the coordinates of the point of the elliptic curve, the difference of coordinates of which is the position of the symbol, that is, in the clear, the cipher does not contain the coordinates of the message points. We also see that all points of the text give the check function a value of zero, that is, all points are points of an elliptic curve

**Conclusion.** The development of encryption and its methods has led to their widespread prevalence. Now it is not difficult for the end user to encrypt a partition on a hard disk or correspondence and establish a secure

---

**ICT, Electronics, Programming, Geodesy**

connection to the Internet. Due to the fact that encryption and other information technologies penetrate our everyday lives, the number of computer crimes is growing. One way or another, encrypted information is an object of protection, which, in turn, must be subject to legal regulation.

## REFERENCES

1. Gdanov O.N., Zolotarev B.B. Methods and means of cryptographic information protection, 167p.
2. Bolotov A.A., Gashkov S.V., Frolov A.B., Chasovskih A.A. An elementary introduction to elliptical cryptography.
3. Recommended Elliptic Curves for Government Use.
4. SEC 2/ Recommended Elliptic Curves Domain Parameters.