УДК 003.26

МОДИФИЦИРОВАННОЙ МЕТОД ШИФРОВАНИЯ ТЕСТОВЫХ ДАННЫХ ЭЛЛИПТИЧЕСКИМИ КРИВЫМИ С ИСПОЛЬЗОВАНИЕМ УНИКАЛЬНОЙ АЛФАВИТНОЙ СТРОКИ-КЛЮЧА.

П.Р. СИНИЦА
(Представлено: канд. физ.-мат. наук., доц. Д.Ф. ПАСТУХОВ)

В статье представлена математика эллиптических кривых. А также вывод формул сложения и удвоение эллиптические точек. Представлено описание алгоритма шифрования и дешифрования. Показана работа разработанной программы на базе математики эллиптических кривых в консоли.

Ключевые слова: *эллиптическая кривая, шифрование, дешифрование, консоль, абелева группа, тестирование, формула сложения, формула удвоения, ключ.*

Введение. Эллиптическая криптография – раздел криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями. Основное преимущество эллиптической криптографии заключается в том, что на сегодняшний день неизвестно существование субэкспоненциальных алгоритмов решения задачи дискретного логарифмирования. Роль основной криптографической операции выполняет операция скалярного умножения точки на эллиптической кривой на данное целое число, определяемое через операции сложения и удвоения точек эллиптической кривой. Последние, в свою очередь, выполняются на основе операции сложения, умножения и инвертирования в конечном поле, над которыми рассматривается кривая. Особый интерес к криптографии эллиптических кривых обусловлен теми преимуществами, которые дают ее применение в беспроводных коммуникациях – высокое быстродействие и небольшая длина ключа.

Математика эллиптических кривых. В криптографических методах используют эллиптические кривые над полем целых чисел с характеристикой поля r = 2 либо более $r > 3$. В дальнейшем мы будем рассматривать поле целых чисел с характеристикой $r > 3$.

Криптографические кривые с характеристикой поля r > 3 имеют канонический вид

$$y^2 = x^3 + ax + b, \tag{1}$$

где a, b – целочисленные коэффициенты кривой;

p – простое достаточно большое число.

Как видно из формулы (1), если точка с координатами (x, y) удовлетворяет уравнению (1), то уравнению (1) удовлетворяет также и точка с (x, $-y$). Под эллиптической кривой понимают геометрическое множество точек (1) дополненное бесконечно – удаленной точкой.

Следующее число, называемое дискриминантом кривой: $\Delta = -16(4a^3 + 27b^2)$, не должно быть равным нулю (в этом случае отсутствуют точки самопересечения и точки возврата). Если дискриминант положителен $\Delta > 0$, то график имеет 2 части, если $\Delta < 0$, то одну часть.

На множестве точек эллиптической кривой определяют группу по сложению точек эллиптической кривой (раздел математики называется алгебраической геометрией). Суммой двух точек э. к. P, Q называется третья точка R , лежащая на прямой PQ и эллиптической кривой одновременно, и обозначается как $R = P + Q$, т.е. $-R + P + Q = 0$.

Операцией группового сложения называют 3 точки э. к., удовлетворяющих уравнению

$$R' + P + Q = 0. \tag{2}$$

Откуда видно, что $R' = -R$ (R', R – элементы взаимно обратные по групповой операции). С другой стороны, прямая параллельная координатной оси у, пересекает ровно 2 точки эллиптические кривые (зеркально симметричные относительно оси х) и бесконечно удаленную точку (в противоположных направлениях), следовательно, взаимно обратные точки эллиптические кривые R', R – имеют координаты (x, y) и (x, $-y$) соответственно. Единицей по групповому сложению определяют геометрически бесконечно удаленную точку и обозначают 0. Итак, для групповой операции по сложению необходимо провести секущую через точки P, Q и зеркально отобразить точку R, $R' = -R$.

Возможны частные случаи:

1) $P = Q$ – секущая прямая вырождается в касательную $R' + 2P = 0$

2) $P + Q + 0 = 0 <=> P = -Q$ точки P, Q (зеркально симметричные) имеют одинаковые абсциссы. Следующей точкой по сложению выбирают точку $Q + 0 = Q$ (образующий элемент абелевой группы).

3) $P + P + 0 = 0 <=> P = 0$ – секущая прямая одновременно является вертикальной прямой и касательной.

Криптография использует конечные циклические абелевые группы с порождающим элементом *G*. При этом любую точку эллиптической кривой циклической группы $1 \le k \le$ n0 получают по формуле: $P_k = (GG \dots G)$. Порядком группы точек эллиптической кривой называется число n0, такое что $P_{n0} = 0$ – нулевой элемент группы. Зная порождающий элемент группы *G*, можно составить таблицу всех точек эллиптической кривой, при сложении точек с порядком $k >$ n0 все точки периодически повторяются: $P_k = P_{k-n0*s}$, где $1 \le k - n0 * s \le n0 - 1$, s ϵN. В зависимости от общей ситуации частных случаев 1), 2), 3) координаты точек эллиптической кривой вычисляют по формулам (индексы 1 и 2 соответствуют точкам *P*, *Q* соответственно):

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

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

Вывод формул (3) и (4)

Угловой коэффициент прямой проходящий через 2 точки равен: $k = \frac{y_2 - y_1}{x_2 - x_1} = \frac{y - y_1}{x - x_1}$, где точка прямой (x, y) является скользящей по прямой. Для точек $1(x_1, y_1)$, $2(x_2, y_2)$, (x, y) получим:

$$y^2 = x^2 + ax + b,$$
$$y_1^2 = x_1^2 + ax + b,$$
$$y_1^2 = x_2^2 + ax_2 + b.$$

Вычтем $(y_2 - y_1)(y_2 + y_1) = (x_2 - x_1)(x_2^2 + x_1x_2 + x_1^2) + a(x_2 - x_1)$, откуда

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

$k = \frac{y - y_1}{x - x_1}, k(y + y_1) = (x^2 + x_1x + x_1^2) + a,$ и последняя формула

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

Вычтем из третьей формулы вторую, получим $k(y_2 - y_1) = x(x_2 - x_1) + (x_2 - x_1)(x_2 + x_1)$

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

Для координаты $y = y_1 + k(x - x_1) = y_1 + k(k^2 - 2x_1 - x_2)$. Остается вспомнить, что для групповой операции нужно выбрать зеркальную точку:

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

Таким образом формула (3) доказана.

В случае перехода секущей в касательную получим $x_2 = x_1$, $x = k^2 - 2x_1$

Далее дифференцируем уравнение 1) по *x*:

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

Из формулы (5) получим $(x, -y) = (k^2 - 2x_1, -y_1 + k(-k^2 + 3x_1)), k = \frac{3x_1 + a}{2y_1}$. Таким образом, доказана формула (4).

Циклическую группу образуют из множества точек эллиптической кривой (уравнение (1), связанных геометрической групповой структурой (формулы (3), (4), дополняют полевой целочисленной структурой по модулю простого числа *p*, т.е. вместо (1) решают сравнения

$$y^2 = x^3 + ax + b(\mathrm{mod}\ p) \tag{6}$$

В конечном итоге мы пользуемся формулами (3), (4) и (6), получая последовательно все точки эллиптической кривой циклической абелевой группы.

Как видно из формул 3) и 4) координаты точек эллиптической кривой являются рациональными числами, если первые 2 точки кривой также рациональные, т.е. геометрическая групповая операция оставляет координаты точек рациональными и дальше. Анализ формул (3) и (4) показывает, что если угловой коэффициент прямой принимает целочисленные значения, то координаты x, y будут и дальше целыми. Таким образом, необходимо решить сравнение:

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

Краткое описание алгоритма построения последовательности точек:

1) Находим обратный элемент в (7) к $2y_1$, либо к $x_2 - x_1$.
2) Находим числа $k_1 = (y_2 - y_1) \bmod p * (x_2 - x_1)^{-1} \bmod p$, либо $k_1 = (3x_1^2 + a), \bmod p * (2y_1)^{-1} \bmod p$.
3) Находим числа

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

Либо по формулам:

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

Описание алгоритма шифрования и дешифрования. Формулу шифрования и дешифрования выглядит следующим образом: (*kG, Pm + k * Pb*) (шифрование) → *Pm + k * nb * G – nb * k * G = Pm* (дешифрование), где *nb* – закрытый ключ абонента *b*, а *Pb* открытый ключ абонента *b*.

Сообщение(число) должно быть равно разности x координаты и y координаты точек эллиптической кривой. Поскольку это возможно не для всех остатков по модулю простого числа *p*. То мы создаем свою собственную алфавитную строку, которая одновременно является и дополнительным ключом шифрования, в котором есть все буквы латинского алфавита и все цифры, расположенные по порядку как в английском алфавите или не по порядку. Кроме того, приходится делать пробелы, чтобы заполнить их символом звездочка. Идея заключается в следующем. Нужно расположить все буквы и цифры в алфавитной строке на тех позициях (порядковый номерах), для которых существует точка эллиптической кривой, разность координат которой равна номеру позиции буквы в алфавитной строке. Таким образом мы о отображаем номера всех букв в алфавитной строке в точки эллиптической кривой. Пример алфавитной строки: **b*a ***cdefghi * jkl **mnopqrs**tuvwxyz01*2**3456789***. Далее из другой строки-слова по символам считываются буквы и записываются в свой массив. Далее сравниваются очередной символ слова и символы алфавитной строки. Как только произошло совпадение букв, символу слова сопоставляется номер позиции в алфавитной строке расположения этого символа и соответствующая ему точка эллиптической кривой, разность координат которой равна данной позиции символа в алфавитной строке. При дешифровании по найденной точке нужно вычесть ее x и y координаты и считать в алфавитной строке символ с данной позицией и записать эту букву алфавита на выходе. Алфавитные строки определяются экспериментально, чтобы все буквы и знаки препинания, числа английского алфавита шифровались и дешифровались однозначно с помощью эллиптической криптографии.

Тестирование программы в консоли. Для тестирования шифрования данных введем фразу с латинским шрифтом Полоцкий государственный университет 2019: «polotsk state university 2019» с длиной

строки *nn* = 29. Результат ввода текста, параметры эллиптической кривой $a = -1$, $b = 188$, $p = 751$, открытый ключ (*kx, ky*) = (201, 5) приведены на рисунке 1.

На рисунке 2 мы видим результат шифрования и дешифрования. Каждому исходному символу текста соответствует четыре целые координаты двух точек эллиптической кривой, расположенных в одной строке. Для удобства ввода и построчного считывания тот же шифр в один столбец записывается в текстовый файл *balka1.txt*. Мы видим полное совпадение шифра на двух этапах.

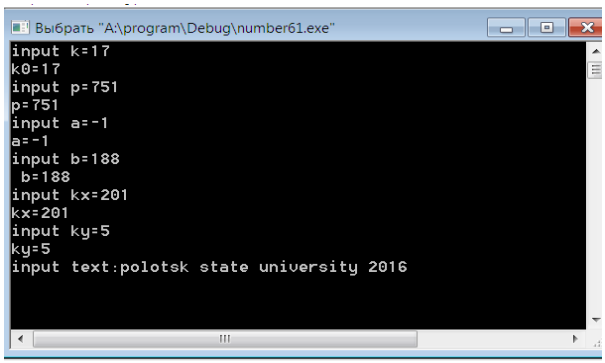

Рисунок 1. – Ввод данных в программу

Кроме того, видно также, что вводимое в программу случайное число *k* = 17 на рисунке 1 и записанное программой в текстовый файл *balka2.txt* также совпадают.

В ходе работы программы составляется протокол шифрования по каждому шифруемому входному символу. Функция проверки $prov(x_1, y_1, a, b, p)$ осуществляет принадлежность каждой проверяемой точки с координатами (x_1, y_1) эллиптической кривой с параметрами a, b, p. Если точка принадлежит эллиптической кривой, то программа проверки возвращает число 0, в противном случае возвращается другое целое число. Принадлежность точек данной эллиптической кривой проводится во многих частях программы и отсутствие принадлежности точки кривой сообщается в протоколе сообщений немедленно. В протоколе шифрования указываются координаты точки эллиптической кривой, соответствующей каждому входному символу и разность координат точки *x* – *y*, которая равна положению исходного символа в алфавитной строке. Например, по точке эллиптической кривой с координатами (*xm, ym*) мы можем определить $(xm, ym) = (680, 657)$, $des = xm - xy = 680 - 657 = 23$ исходный символ, используя алфавитную строку (нумерация символов в алфавитной строке начинается с нуля, поэтому $des = 23$ соответствует 24 символу, т.е. латинской букве *p* (рисунок 2 снизу).

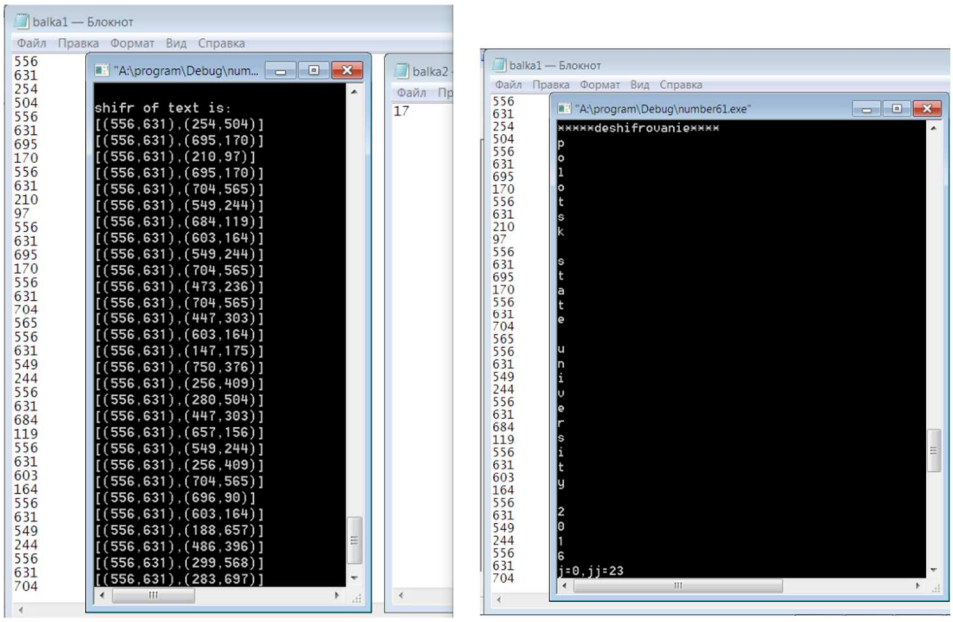

Рисунок 2. – Результат выполнения операции шифрования(слева) и дешифрования(справа)

Действительно, фраза «polotsk state university 2019» начинается с буквы *p*.

Второй символ $(xm, ym) = (266, 244)$, $des = xm - xy = 266 - 244 = 22$ соответствует 23 по счету символу в алфавитной строке, т.е. латинской букве o, что соответствует второй букве в слове polotsk. Из консоли видно, что шифр имеет другие координаты, чем координаты точки эллиптической кривой, разность координат которой есть позиция символа, то есть в открытом виде шифр не содержит координат точек сообщения. Так же мы видим, что все точки текста дают функцией проверки значение ноль, то есть все точки являются точками эллиптической кривой (рисунок 2 снизу).

Заключение. Развитие шифрования и его методов привело к их широчайшей распространенности. Сейчас для конечного пользователя не составляет труда зашифровать раздел на жестком диске или переписку и установить защищенное соединение в интернет. В связи с тем, что шифрование и другие информационные технологии проникают в наш быт, растет число компьютерных преступлений. Зашифрованная информация так или иначе представляет собой объект защиты, который, в свою очередь, должен подвергаться правовому регулированию.

Имея длинную кодовую строку ключ можно увеличить пространство ключей до такой степени, что их перебор даже при известных параметрах кривой a, b, p и образующего элемента группы G, становится невозможным для злоумышленника. Даже для алфавита из 36 символов – 26 букв английского алфавита и 10 цифр, минимальная кодовая строка имеет число переборов 36! = 3.7 × 1041. Пусть суперкомпьютер может анализировать шифры со скоростью миллиард шифров в секунду. При этом понадобится времени порядка 3,7 × 1032 с = 10^{25} лет. Что реально невозможно для разгадывания кодовой строки методом перебора даже при известных параметрах эллиптической кривой и образующем элементе группы G. Основываясь на этих фактах данный алгоритм обеспечит надежное шифрование данных.

ЛИТЕРАТУРА

1. Березин Б.В., Дорошкевич П.В. Цифровая подпись на основе традиционной криптографии: вып. 2 – М : МП Ирбис – II, 1992 – 202 с.
2. Бутакова Н.Г., Семененко В.А., Федоров Н.В. Криптографическая защита информации: учеб. пособие для вузов. – М. : Изд-во МГИУ, 2011. – 316 с.
3. Жданов О.Н., Чалкин В.А. Эллиптические кривые: Основы теории и криптографические приложения. – М. : Книжный дом ЛИБРИКОМ, 2013. – 200 с.
4. Жданов О.Н., Золотарев В.В. Методы и средства криптографической защиты информации. – 167 с.
5. Болотов А.А., Гашков С.Б., Фролов А.Б., Часовских А.А. Элементарное введение в эллиптическую криптографию.
6. Recjmmended Eliptic Curves for Govement Use.
7. SEC 2/ Recommended Eliptic Curves Domain Parametres.