УДК 681.3

ИСПОЛЬЗОВАНИЕ ЭЛЛИПТИЧЕСКИХ КРИВЫХ В ЗАЩИТЕ ИНФОРМАЦИИ

Куржеевский Игорь Владимирович, Филимонова Анастасия Викторовна, Бродовская Виолета Владимировна

Академия военно-морских сил имени П. С. Нахимова, Украина

Аннотация

В данной работе рассматривается алгоритм шифрования основанный на операции вычитания точек эллиптической кривой и методе замены, который может быть использован для решения задач защиты информации от несанкционированного доступа в телекоммуникационных сетях.

In this paper we consider the encryption algorithm based on the subtraction of the elliptic curve method and the replacement, which can be used to solve the problems of information protection against unauthorized access to telecommunications networks.

Введение

Шифрование — способ преобразования открытой информации в закрытую, и обратно. Качественное шифрование обеспечивает безопасность информации, а также аутентификацию. Эллиптические кривые являются одним из основных объектов изучения в современной теории чисел и криптографии. Например, они были использованы Эндрю Уайлзом (совместно Ричардом Тейлором) в доказательстве Великой теоремы Ферма. В частности, на эллиптических кривых основан стандарт цифровой подписи ДСТУ 41.45-2002 и ГОСТ Р 34.10-2001.

Основная часть

Эллиптическая кривая — математический объект [1], который может быть определен над любым полем и описывается кубическим уравнением следующего вида:

$$y^2 + cxy + dy = x^3 + ex^2 + fx + g$$

где c, d, e, f и g являются действительными числами, удовлетворяющими некоторым условиям. Ньютон доказал, что над полем действительных чисел любую эллиптическую кривую можно преобразовать, с помощью замены координат к виду(формула Вейерштрасса):

$$Y^2 = X^3 + aX + b$$

Чтобы найти точки пересечения эллиптической кривой с осью абсцисс необходимо решить кубическое уравнение с помощью формул Кардано.

$$X^3 + aX + b = 0$$

Дискриминант этого уравнения имеет вид:

$$D = \left(\frac{a}{3}\right)^3 + \left(\frac{b}{2}\right)^2$$

Если D<0, то уравнение имеет три различных действительных корня α, β, γ.

Если D=0,то уравнение имеет три действительных корня, предположим α, β, β, дваизнихравны.

Если D>0, то уравнение имеет один действительный корень αидвакомплексносопряженных.

Точки эллиптической кривой можно складывать. Сложение точек эллиптической кривой равносильно умножению чисел в неэллиптической криптографии. Сумма двух точек, в свою очередь, также принадлежит эллиптической кривой и имеет координаты, которые вычисляются по следующим формулам:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \text{если} P \neq Q$$

$$\lambda = \frac{3x_1^2 + a}{2y_1}, \text{если} P = Q$$

где λ– угловой коэффициент секущей, аx_1, x_2, y_1, y_2-координаты точек $P = (x_1, y_1), Q = (x_2, y_2), P + Q = T(x_3, y_3)$.

$$x_3 = \alpha^2 - x_1 - x_2 \, mod \, p$$

$$y_3 = \alpha * (x_1 - x_3) - y_1 \, mod \, p$$

Математическое свойство, которое делает эллиптические кривые полезными для криптографии[1], состоит в том, что если взять две различных точки на кривой, то соединяющая их хорда пересечет кривую в третьей точке (так как мы имеем кубическую кривую). Зеркально отразив эту точку по оси X, мы получим еще одну точку на кривой (так как кривая симметрична относительно оси X). Если мы

обозначим две первоначальных точки как P и Q, то получим последнюю "отраженную" точку P+Q. Это сложение удовлетворяет всем известным алгебраическим правилам для целых чисел.

Операция вычитания точек эллиптической кривой реализуется следующим образом: предположим, что необходимо найти разность точек R и Q. Для этого необходимо отобразить точку R симметрично оси OX и получить точку R1. Складывая точки R1 и Q получаем их сумму — точку P1, затем следует отобразить точку P1 симметрично оси OX и в результате получаем точку P, являющуюся разностью точек R и Q.

Рассмотрим этапы работы алгоритма:

1. Выбираем ЭК, в соответствии с рекомендациями стандарта ДСТУ 41.45-2002, и модуль по которому будем осуществлять вычисления.

2. Для каждого сеанса связи создается новый алфавит следующим образом:

2.1. Два генератора ПСП ГПСП №1 с ключом k1 и ГПСП №2 с ключом k2 генерируют случайные числа, значение которых берется по заданному модулю. Затем происходит проверка принадлежности точки, имеющей сгенерированные координаты (X, Y) заданной ЭК. Если точка принадлежит ЭК, то ей ставится в соответствие некоторый символ алфавита, таким образом, происходит генерация алфавита с последующей проверкой уникальности каждого символа.

2.2. Созданный алфавит записывается в двухмерный массив заданного размера, например массив 16*16.

3. Считываем из файла исходный текст подлежащий шифрованию.

4. Задаем количество случайных символов, которыми будет "разбавлен" исходный текст.

5. Генерируем случайные символы.

6. Создаем символьный одномерный массив с длиной, равной длине файла плюс количество сгенерированных случайных символов.

6.1. Создаем контрольный массив такого же размера и заполняем его 1.

7. Перемешивание символов исходного текста и случайных символов происходит следующим образом:

7.1. С помощью ГПСП №3 с ключом k3 генерируем случайное число в заданном диапазоне, с помощью контрольного массива проверяем, свободна ли ячейка с данным номером, если да, то записываем текущий символ в данную ячейку памяти, при этом в контрольном массиве отмечаем, например, с помощью 0, что данная ячейка занята. Этот процесс продолжается до тех пор, пока не будут переставлены все символы исходного текста и случайные символы.

8. Под управлением ГПСП №4 с ключом k4 и ГПСП №5 с ключом k5 осуществляем циклические сдвиги столбцов и строк двухмерного массива, с записанным в нем алфавитом.

9. Очередной символ исходного текста заменяется символом перемешенного двухмерного массива, стоящем на том же месте, что и исходный символ в алфавите. Затем символу ставятся в соответствие координаты точки на ЭК, согласно, созданного алфавита.

10. Считываем из ключевого файла очередной символ «гаммы».

11.Складываем точки эллиптической кривой, соответствующие символу исходного текста и символу «гаммы»; 14.Результат шифрования записываем в файл.

Секретными ключами в данной системе шифрования являются ключи к генераторам ПСП k1, k2, k3, k4, k5 и символы «гаммы».

Для расшифрования необходимо:

1. Считать из соответствующих файлов очередной символ зашифрованного текста и символ "гаммы".

2. Найти разность точек эллиптической кривой, соответствующих символу зашифрованного текста и символу "гаммы"и записать полученное значение в одномерный массив.

3. С помощью ГПСП №3 с ключом k3 делаем обратные перестановки элементов одномерного массива.

4. Случайные символы отбрасываются, а символы исходного текста записываются в файл.

Предложенный алгоритм на эллиптической кривой был реализован в среде программирования Aribasw и на языке C(SHARP) и в ходе тестирования показал правильные результаты шифрования и расшифрования различных текстов. Аналогичных алгоритмов шифрования, использующих операцию вычитания точек на эллиптической кривой, при поиске в сети Internet авторы не обнаружили. Криптостойкость данного алгоритма основывается, прежде всего, на качестве "гаммы в качестве которой можно использовать любой другой текстовый документ, но для представления символов этого документа необходимо сгенерировать другой алфавит. Целесообразно после шифрования определенного числа символов исходного текста создавать новые алфавиты, как для символов исходного текста, так и для символов "гаммы".

Список использованных источников:

1. Рябко Б.Я Криптографические методы защиты информации: учеб. [Для вузов]/ Б.Я.Рябко, А.Н.Фионов;- М.: Горячая линия-Телеком, 2005.-229с