УДК

Введение в эллиптическую криптографию

Патюпин М.С.1, студент гр.250505

Белорусский государственный университет информатики и радиоэлектроники1

г. Минск, Республика Беларусь

Смирнова И.А. – ассистент кафедры ВМ

**Аннотация.** Математические свойства эллиптических кривых, алгоритм Диффи-Хеллмана его описание, числовая и программная реализация. Принцип работы алгоритма ECDSA и подбор параметров эллиптической кривой.

**Ключевые слова.** Алгоритм ECDSA, алгоритм Диффи-Хеллмана, эллиптические кривые, эллиптическая криптография.

Оглавление:

1. Введение

1.1 Основные плюсы и минусы эллиптической криптографии

2. Математические свойства эллиптических кривых

2.1 Определение эллиптических кривых

2.2 Операции над точками эллиптической кривой

2.2.1 Сложение точек

2.2.2 Вычитание точек

* + 1. Умножение точки на число

1. Алгоритмы на эллиптических кривых
   * 1. Алгоритм Диффи-Хеллмана.
     2. Числовая реализация
     3. Программная реализация

3.2.1 Алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm)

1. **Введение**Эллиптические кривые в криптосистемах предложили использовать Нил Коблиц и Виктор Миллер еще в 1985 году, сейчас мы можем наблюдать их использование в электронной подписи Bitcoin, в сетевых протоколах SSH и TLS, в электронной подписи(Citisen Card) граждан некоторых стран (Австрия). В Беларуси был принят стандарт для решения задач связанных с цифровой подопью на основе эллиптических кривых в 2013 году[1].
   1. **Основные плюсы и минусы эллиптической криптографии**

Основные плюсы эллиптической криптографии:

* Более высокая стойкость при равной трудоемкости по сравнению с обычными криптосистемами[2].
* Меньший размер ключа чем в асимметричной криптографии. Криптостойкость достигаемая в алгоритме алгоритме RSA с использованием ключа в 3072-байт, на эллиптических кривых используется с размером ключа в 256 байт[2].
* Возможность использоваться в устройствах с ограниченными вычислительными ресурсами[3].
* Сложность атак: атаки на системы, защищенные эллиптической криптографией, требуют значительного объема вычислений и времени.

Основные минусы эллиптической криптографии:

* Вероятность появления субэкспоненциальных алгоритмов решения задачи дискретного логарифмирования. При их появлении алгоритмы шифрования на эллиптических кривых будут легко решаемы[4].
* При переходе на алгоритмы шифрования основанных на эллиптических кривых велика вероятность выявления большого числа ошибок и уязвимостей, которые уже отработаны для более привычных методов шифрования.

**2. Математические свойства эллиптических кривых**

**2.1 Определение эллиптических кривых**

Для начала определим эллиптическую кривую как алгебраическую кривую, те каким-то множеством точек которые удовлетворяют следующему уравнению: (1)

(1)

где x, y – переменные, , , , , – коэффициенты. Так-же уравнение(1) можно представить как(2):

(2)

где x, y – переменные, a, b– коэффициенты. Функция (2) называется функцией Вейерштрасса, не все эллиптические кривые можно представить таким уравнением, но для большинства использующихся в криптографии он корректен.

Так как график кривой параллелен оси абсцисс, чтобы найти точки, являющиеся корнями, нужно решить уравнение третьей степени (3).

(3)

Здесь можно использовать формулу Кардано. Дискриминант вычисляется по формуле (4)

(4)

При дискриминанте меньше нуля, уравнение (3) имеет три разных решения a, b, z; при дискриминанте равном нулю, уравнение (3) имеет три корня, a, b, c, два из которых одинаковые, при дискриминанте больше нуля, уравнение (3) имеет одно решение a и два комплексно сопряженных. Графики по результатам вычислений представлены на рисунках 1-3.

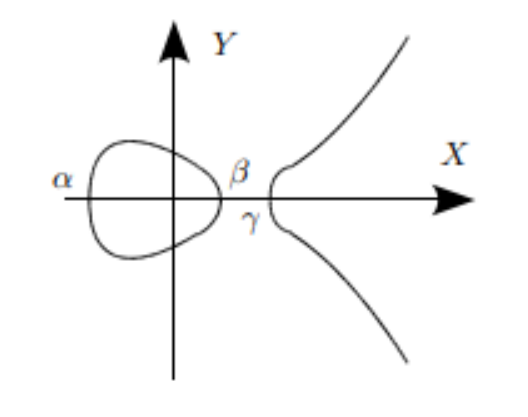


Рисунок 1 – Кривая с D < 0

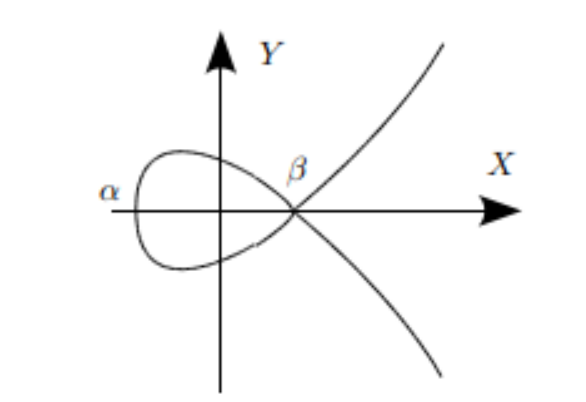


Рисунок 2 – Кривая с D = 0

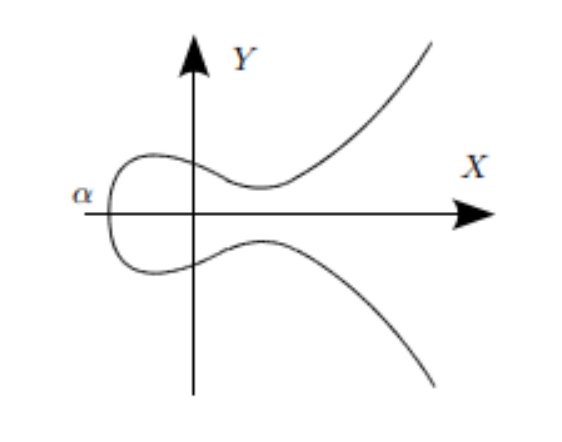


Рисунок 3 – Кривая с D > 0

Эллиптические кривые дискриминант которых не равен нулю (рисунок 1, 3) называются несингулярными, соответственно если дискриминант равен нулю, то сингулярные. Последние используются редко в связи с снижением криптостойкости алгоритмов и протоколов.

**2.2 Операции над точками эллиптической кривой**

**2.2.1 Сложение точек**

Пусть координаты точки P, а координаты точки Q, для нахождения точки R – суммы точек P и Q, необходимо провести прямую через эти точки P и Q, получаем пересечение прямой с кривой в точке R’ и отразить эту точку относительно ОХ(рис. 1). То есть

, (5)

Для нахождения координат точки R найдем коэффициент α,

, далее ,

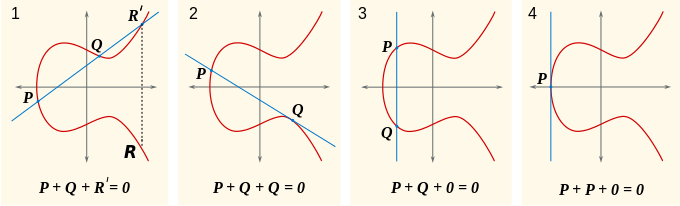


Рисунок 4.1-4.4

Для случая если прямая пересекает кривую только в двух местах и пересекает оси (рис. 4.2), то выполняется следующие уравнение (6), соответственно (7)

Третий случай если прямая пересекает кривую в двух местах и параллельна оси ординат (рис. 4.3):

(8)

Четвертый если прямая касается кривой в одной точке (рис. 4.4):

(9)

**2.2.2 Вычитание точек**

Пусть координаты точки P, а координаты точки Q, – координаты точки -Q. Вычитание точек, это сложение точек с обратной точкой(10).

(10)

**2.2.3 Умножение точки на число**

Пусть P – точка на эллиптической кривой, n – любое целое число, Q = n \* P – произведение точки P на число n. Для нахождения Q будем использовать алгоритм быстрого умножения.

Разберем алгоритм умножения, пусть n = 37:

1. Разложим n по степеням двойки:

n = 37 = 32 + 4 + 1

1. Раскладываем произведение n на P:

Q = 37\*P = 32\*P + 4\*P + P

Рассмотрим возможные слагаемые:

1\*P = P

2\*P = P + P

4\*P = 2\*P + 2\*P

8\*P = 4\*P + 4\*P

16\*P = 8\*P + 8\*P

32\*P = 16\*P + 16\*P, можем заметить, что для вычисления Q потребуется 7 сложений.

1. **Алгоритмы на эллиптических кривых**
   * 1. **Алгоритм Диффи-Хеллмана**

Рассмотрим пример. Предположим, существует два абонента: Алиса и Боб. Обоим абонентам известны некоторые два числа �  и �, которые не являются секретными и могут быть известны также другим заинтересованным лицам. Для того, чтобы создать неизвестный более никому секретный ключ, оба абонента генерируют случайные числа: Алиса — число �, Боб — число �. Затем Алиса вычисляет остаток от деления (11):

(11)

и пересылает его Бобу, и Боб вычисляет остаток от деления (12):

(12)

и передаёт Алисе. Предполагается, что злоумышленник может получить оба этих значения, но не модифицировать их. На втором этапе Алиса на основе имеющегося у неё и полученного по сети � вычисляет значение (13):

(13)

Боб на основе имеющегося у него � и полученного по сети � вычисляет значение (14):

(14)

Можем видеть что, у Алисы и Боба получилось одно и то же число (15):

(15)

Его они могут использовать в качестве секретного ключа.

Работа алгоритма показана на рисунке.

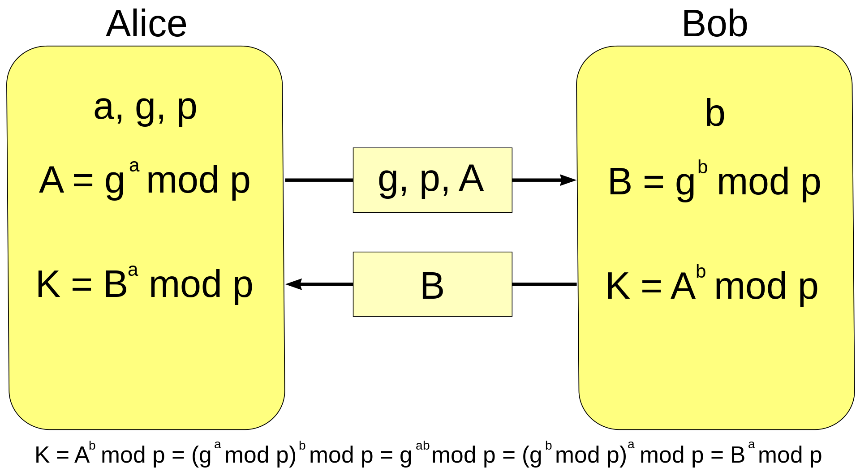


Рисунок 5 - Работа алгоритма.

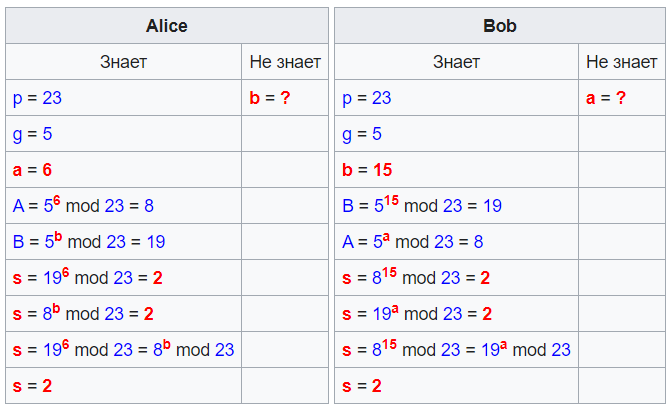
При работе алгоритма каждая сторона [5]:

1. Генерирует случайное натуральное число  — закрытый ключ.
2. Совместно с удалённой стороной устанавливает открытые параметры �  и .
3. Вычисляет открытый ключ , используя преобразование (11) над закрытым ключом.
4. Обменивается открытыми ключами с удалённой стороной.
5. Вычисляет общий секретный ключ  (15), используя открытый ключ удаленной стороны  и свой закрытый ключ .

* + 1. **Числовая реализация**

Пусть s = 2 - секретный ключ, g = 5 - первообразный корень по модулю р, p = 23 - открытое простое число, a = 6 - секретный ключ Алисы, A = ga mod p = 8 - открытый ключ Алисы, b = 15 - секретный ключ Боба, B = gb mod p = 19 - открытый ключ Боба.

Тогда, пройдя и записывая каждый шаг в алгоритме Диффи-Хеллмана, составим следящую таблицу:



* + 1. **Программная реализация**

Перейдем к программной реализации алгоритма. Алгоритм Диффи-Хеллмана реализован на языке С, в среде разработки CLion.

Создаем функцию для вычисления (в нашем случае уравнения 11,12 рис. 6):

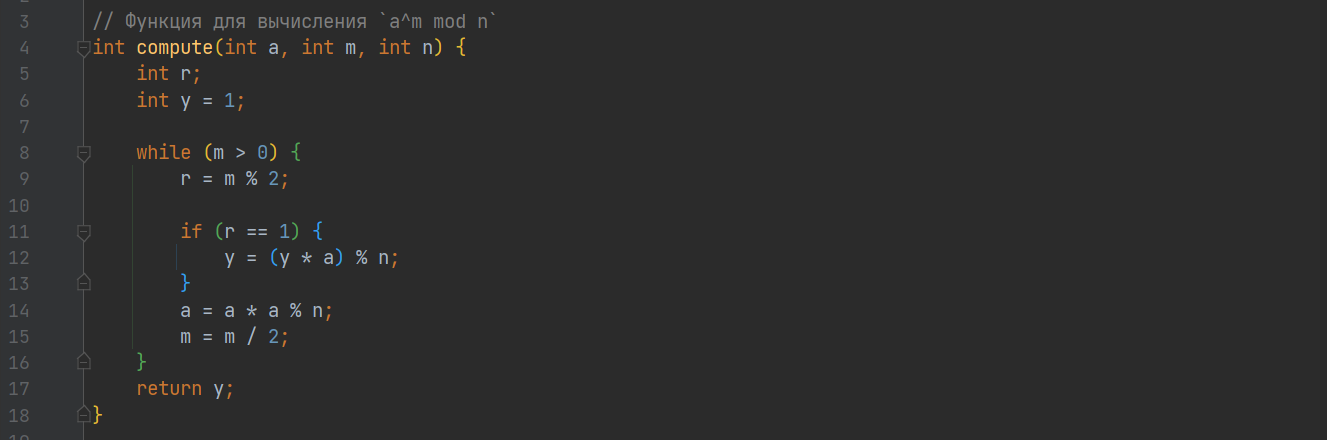


Рисунок 6

Объявляем следующие значения согласно числовой реализации: g - первообразный корень по модулю р, p - открытое простое число, a - секретный ключ Алисы, A - открытый ключ Алисы, b - секретный ключ Боба, B - открытый ключ Боба. И действуем согласно алгоритму (рис.7).

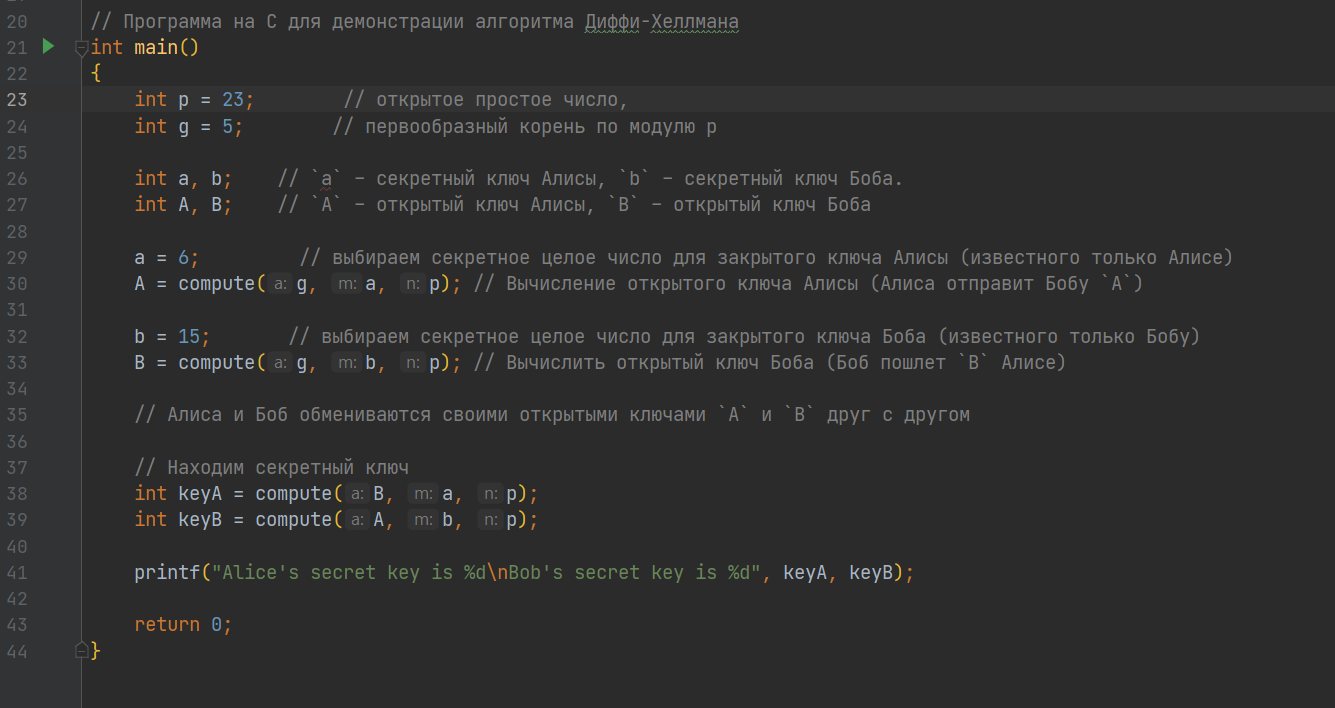


Рисунок 7.

Результат выполнения программы (секретный ключ) (рис.8).

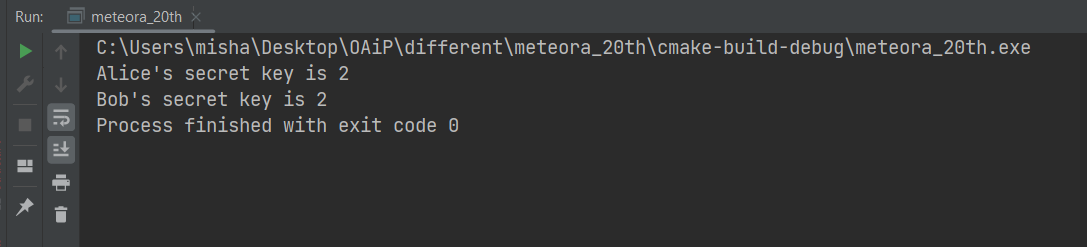


Рисунок 8 – Результат выполнения программы.

**3.2.1 Алгоритм ECDSA (Elliptic Curve Digital Signature Algorithm)**

ECDSA — алгоритм с открытым ключом, использующийся для построения и проверки электронной цифровой подписи(ЭЦП). Алгоритм начинается с выбора параметров эллиптической кривой, для облегчения этой задачи национальным институтом стандартов и технологий (NIST), был составлен список эллиптических кривых с уже известным количеством точек, которые рекомендовано использовать в схемах ЭЦП.

Кривая в стандарте описывается набором из 6 параметров D=(p,a,b,G,n,h), где

p – простое число, модуль эллиптической кривой, данное число относится к обобщенным числам Мерсенна, это означает, что его можно представить как сумму различных степеней двойки.

a, b – задают уравнение эллиптической кривой(2).

G – точка эллиптической кривой большого порядка.

n – порядок точки G;

h – параметр, называемый кофактор. Определяется отношением общего числа точек на эллиптической кривой к порядку точки G. Данное число должно быть как можно меньше[5].

Вот несколько кривых рекомендованных NIST (табл. 2, 3).

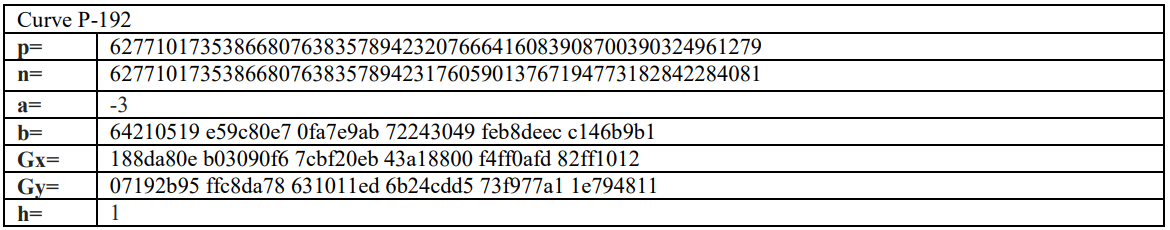


Таблица 2 – Curve P-192

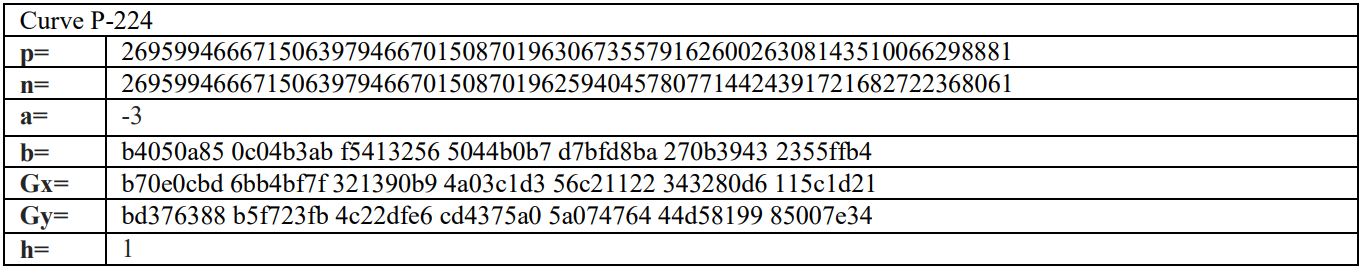


Таблица 3 – Curve-224

Точка G принадлежит эллиптической кривой. Соответственно для нее выполняется равенство(2), из которого можем вычислить (16):

(16)

Формирование и проверка подписи

Рассмотрим алгоритм обмена ключами. Пусть пользователи A и B хотят обменяться ключами, но их трафик прослушивает злоумышленник E. Алгоритм следующий:

1. Пользователь А генерирует случайно число в диапазоне [1; n-1]. Это число его закрытый ключ.

2. Затем A вычисляет и посылает координаты точки пользователю B. – открытый

ключ пользователя A.

3. Пользователь B генерирует случайно число в диапазоне [1; n-1]. Это число его закрытый ключ.

4. Затем B вычисляет и посылает координаты точки пользователю A. – открытый

ключ пользователя B.

5. Пользователь A получает , вычисляет и считает, что – это общий ключ.

6. Пользователь B получает , вычисляет и считает, что – это общий ключ.

Оба пользователя получили один и тот же ключ, потому что

Злоумышленник E видит только и . – открытые ключи пользователей.[5]

**Список использованных источников:**

1. СТБ 34.101.45-2013 АЛГОРИТМЫ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ И ТРАНСПОРТА КЛЮЧА НА ОСНОВЕ ЭЛЛИПТИЧЕСКИХ КРИВЫX
2. Guide to Elliptic Curve Cryptography
3. Шифрование данных на базе эллиптических кривых, Д.Ф. Пастухов Ю.Ф. Пастухов П.Р. Синица
4. Интернет-ресурс: <https://habr.com/ru/articles/692842/>
5. Интернет ресурс: http://habrahabr.ru/post/191240/

UDC

INTRODUCTION TO ELLIPTICAL CRYPTOGRAPHY

Patsiupin M.S.

Belarusian State University of Informatics and Radioelectronics1, Minsk, Republic of Belarus

Surname N.P. – PhD in Physics and Mathematics

**Annotation.** Mathematical properties of elliptic curves, the Diffie-Hellman algorithm, its description, numerical and software implementation. The principle of operation of the ECDSA algorithm and the selection of parameters of the elliptic curve.

**Keywords.** ECDSA algorithm, Diffie-Hellman algorithm, elliptic curves, elliptic cryptography.