Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

«Исследование криптографических алгоритмов на основе эллиптических кривых»

Выполнил:

студент 3 курса 8 группы

специальности ПОИБМС

Романович Н.Р.

Минск 2020

1. **Теоретические сведения**

**Основные этапы генерации ключевой информации на основе ЭК**

Первый этап. Выбор (генерация) ЭК. Обычно он основан на выполнении следующих условий и операций.

1.1. Входными параметрами являются: число l, число р, удовлетворяющее условию 22l-1 <р <22l, р = 3 mod 4, 0 <a <p. Можно использовать некоторое простое число р = 22l – с, где с – небольшое натуральное число.

1.2. Выбирается число b, такое, что 0 <b <p. Таким образом, задана ЭК: Ер (а, b).

1.3. Выбираются порядок q (простое число) и генерирующая точка G, которая задается двумя координатами, например, G = (0, уG).

Дополнительно к рассмотренным действиям стандарт [50] предусматривает использование вспомогательного параметра (s, seed) – произвольное 64битное число.

Для примера в нижеследующей иллюстрации (рис. 11.7) [50] приведены параметры ЭК для двух значений l. (на иллюстрации это – Таблица Б.1 и Таблица Б.2). Здесь нижние индексе в левом столбце обозначают битовую длину числа.

Второй этап*.* Генерация ключевой информации. 2.1. Входными параметрами являются: р, а, b, q и G. 2.2. Генерируется тайный ключ – число d, выбранное из множества {1, 2, …, q–1}. 2.3. Вычисляется открытый ключ – точка Q: Q = dG к открытому ключу также относятся р, а, b, q.

**Использование ЭК в криптографии**

Отметим еще раз, что ЭК в криптографических приложениях обычно используется на этапе генерации либо согласования ключевой информации. Таким образом, можно отметить 3 направления использования ЭК в криптографии:

* в алгоритмах согласования (передача) ключевой информации (на основе идеи Диффи-Хеллмана),
* в алгоритмах асимметричного шифрования/дешифрования сообщений,
* в алгоритмах генерации/верификации ЭЦП.

**Реализация алгоритма Диффи-Хеллмана на основе ЭК**

Рассмотрим наиболее общий случай. Предположим, что Eр – это ЭК над Fр, а Q – заранее определенная и согласованная сторонами А и В точка на E.

Отправитель A выбирает тайное случайное число kA, вычисляет точку РА = kA\*Q и отправляет ее получателю B. B действует аналогично: он случайным образом выбирает число kB, вычисляет случайное число kA, вычисляет точку РВ = kВ\*Q и отправляет результат стороне A.

Общий ключ P = kA\*kB\*Q. Отправитель A вычисляет P путем умножения числа РВ, полученного от получателя B, на его секретное число kA. Похожим образом действует другая сторона.

**Реализация алгоритма зашифрования/расшифрования на основе ЭК**

Вспомним, что процедура предусматривает использование ключей получателя (стороны В). Рассмотрим это на примере алгоритма Эль-Гамаля. Вспомним, что зашифрованное сообщение М или каждый зашифрованный блок (mi) этого сообщения состоят из двух чисел. Вспомним лабораторную работу № 8, где блок шифртекста (ci) в соответствии с (8.9) и (8.10) мы обозначали двумя символами аi и bi и вычисляли как

аi = gk mod p,bi = (yk•mi) mod p.

Поскольку символы, а и b мы зарезервировали в текущей работе для обозначения параметров ЭК, то блок шифртекста сейчас будем обозначать соответственно символами Сi1 и Ci2. При использовании ЭК зашифрование предполагает представление сообщения в виде точки Р (или представления каждого блока сообщения в виде разных точек Рi) ЭК с известной точкой G и известным Q. Соответственно шифртекст – это две точки на той же ЭК: С1 и C2 или Сi1 и Ci2. Предположим, что шифруемое сообщение М – это точка Р на ЭК. Сторона А выбирает некоторое случайное число k и далее выполняет вычисления с использованием открытого ключа стороны В:

С1 = kG, С2 = P + kQ. (11.9)

Получатель для расшифрования сообщения вычисляет:

P = С2 – dC1. (11.10)

Знак «–» в (11.10) означает сложение с инверсией: инверсией по отношению к точке (х, у) является точка (х, –у) на ЭК.

**Реализация ЭЦП на основе ЭК**

Рассмотрим генерацию и верификацию ЭЦП на основе алгоритма DSA и ЭК (EC) – ЕСDSA. Обращаем внимание на то, что используется ключевая информация отправителя (стороны А). Генерация ключей происходит так же, как и в последнем примере. Однако в анализируемом здесь случае во внимание должен приниматься еще один известный параметр ЭК: порядок точки G, т. е. число q.

Краткая характеристика алгоритма генерации и верификации ЭЦП. Полагаем, что отправитель подписывает хеш Н(М) сообщения М.

Генерация ЭЦП.

1. Выбрать число k (1 <k <q), q – порядок точки G.

2. Вычислить точку kG = (х, у), вычислить r = x mod q; при r = 0 изменить k и повторить шаг 2.

3.Вычислить t = k-1mod q (например, на основе расширенного алгоритма Евклида).

4.Вычислить s = (t (H(M) + dr)) mod q; при s = 0 изменить k и повторить алгоритм. Стороне B отсылаются сообщение М и ЭЦП (числа r и s).

Верификация ЭЦП.

Получатель знает алгоритм хеширования, который использовался отправителем, открытый ключ отправителя, с помощью чего выполняет следующие операции над М и полученной ЭЦП (обозначения чисел оставим без изменений).

1. Проверить выполнение условия: 1 <r, s <q; если условие не выполняется, то легитимность подписи не подтверждается, в противном случае – выполняются дальнейшие шаги.

2. Вычисляются Н(М) и w = s–1 mod q.

3. Вычисляются u1 = w Н(М) (mod q), u2 = wr (mod q).

4. Вычисляются Gu1 + Qu2 = (x', y'), v = x' mod q.

5. Сравниваются v и r; если равенство выполняется, подтверждается легитимность подписи и целостность полученного сообщения.

**2. Практическая часть**

В основе задания – ЭК вида у2 = х3 – х + 1 (mod 751): а = –1, b = 1, р = 751, т. е. Е751(–1, 1).

Задание I.

1.1 Найти точки ЭК для значений х, указанных в табл. 11.4



1.2. Разработать приложение для выполнения операций над точками кривой: а) kР, б) Р + Q, в) kР + lQ – R, г) Р – Q + R.

Варианты коэффициентов приведены в табл. 11.5.

В табл. 11.6 указаны координаты точек, над которыми выполняются операции.

Результаты выполнения операций представить в табличной форме.



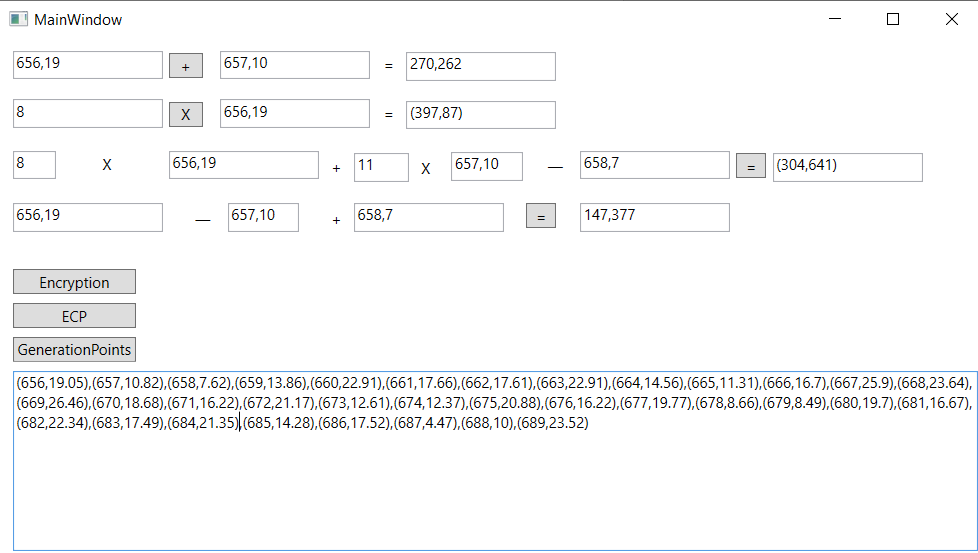


Рисунок 2.1 – Получение результатов выполнения требуемых операций

Задание II.

2.1. Создать оконное приложение для зашифрования/расшифрования собственной фамилии (или имени – по выбору) на основе ЭК, указанной в задании I, для генерирующей точки G = (0, 1). Тайный ключ – в соответствии с вариантом из табл. 11.7.

2.2. Вычислить самостоятельно значение открытого ключа, Q. При этом следует воспользоваться основной формулой (11.8), а также соотношениями (11.3) -(11.5) для случая P = Q; не следует также забывать, что все вычисления производятся по mod 751; см. также пример 5 (вычисление 2Р) и пример 7.

Принять, что шифруемым блоком является один символ сообщения, координаты которого на ЭК соответствуют табл. 11.8 (может быть принята за основу и иная таблица).

Параметры k – по собственному усмотрению.

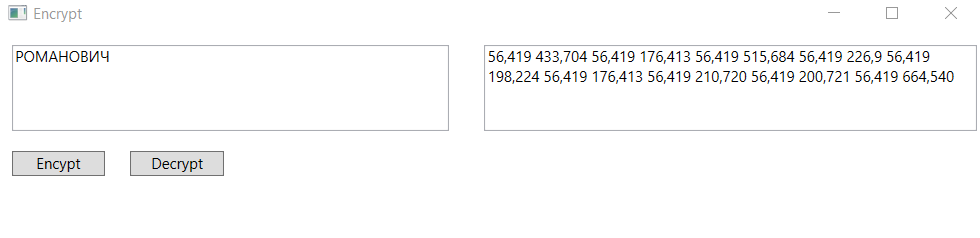


Рисунок 2.2 – Получения результата зашифрования/расшифрования собственной фамилии.

Задание III.

3.1. Создать оконное приложение для генерации/верификации ЭЦП на основе алгоритма ЕСDSA: ЭК Е751(–1, 1) c генерирующей точкой G = (416, 55); порядок точки q = 13. Тайный ключ – в соответствии с вариантом из табл. 11.7. Тайный ключ – в соответствии с табл. 11.9.

3.2. Вычислить самостоятельно значение открытого ключа, Q. При этом следует воспользоваться основной формулой (11.8), а также соотношениями (11.3) -(11.5) для случая P = Q; не следует также забывать, что все вычисления производятся по mod 751; см. также пример 5 (вычисление 2Р) и пример 7. Параметры k – по собственному усмотрению.

3.3. Хешем подписываемого сообщения, (Н(М)), является модуль по основанию 13 координаты х точки ЭК, соответствующей первому символу собственной фамилии, из табл. 11.8. Например, фамилия начинается на букву «Я»: х = 227, тогда 227 mod 13 = 6, значит в данном конкретном случае Н(М) = 6.

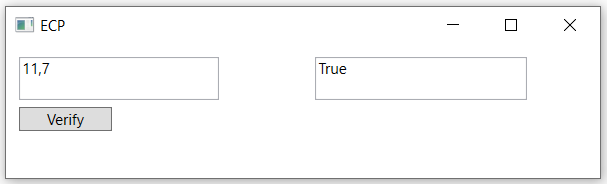


Рисунок 2.2 – Получения результата генерации/верификации ЭЦП.