МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Информационных Технологий

Кафедра Информационных систем и технологий

Специальность 1-40 01 01 Программное обеспечение информационных технологий

Направление специальности 1-40 01 01 10 Программирование интернет-приложений

**ОТЧЁТ К ЛАБОРАТОРНОЙ РАБОТЕ №13:**

по дисциплине «Криптографические методы защиты информации»

Исполнитель

студентка 3 курса группы 5 Шкода Кристина Михайловна

(Ф.И.О.)

Руководитель работы преподаватель Савельева М. Г.

(учен. степень, звание, должность, подпись, Ф.И.О.)

Минск 2023

**Исследование криптографических алгоритмов на основе эллиптических кривых**

**Определение 1.** Эллиптические кривые – математический объект, который может быть определен над любым полем.

**Определение 2.** Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением *у*2 = *х*3 + *aх* + *b*

при этом константы (а и b – вещественные числа) должны удовлетворять условию:

Формула называется уравнением Вейерштрасса, а условие исключает из рассмотрения кривые с особыми точками или особые кривые.

В зависимости от значений a и b ЭК могут принимать на плоскости разные формы.

**Определение 3.** Частью ЭК является бесконечно удаленная точка (также известная как идеальная точка), которую мы обозначим символом О.

**Определение 4.** Группа – непустое множество с определенной на нем бинарной операцией, называемой сложением и удовлетворяющей нескольким аксиомам.

На основе последнего определения мы можем определить группу для ЭК.

**Определение 5.** Группа для ЭК есть непустое множество, элементы которого являются точками ЭК

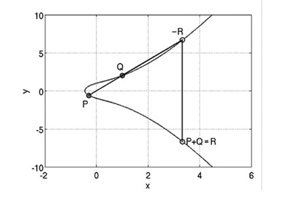


Рисунок 1.1 – Пояснение к операции сложения двух точек *P* и *Q*

эллиптической кривой *у*2 = *х*3 + 2*х* +1 (*а* = 2, *b* = 1)

Что будет, если *P* = *Q*? В этом случае мы можем говорить об операции удвоения точки: *P* + *Р* = 2*Р*. Обобщив (к точке 2*Р* можно прибавить еще раз точку *Р*: 2*Р* + *Р*), сформулируем принцип умножения точки *Р* на целое положительное число n – определяется как сумма n точек *Р: nP* = *P* + *P* + *P* + +…+ *P*.

Скалярное умножение осуществляется посредством нескольких комбинаций сложения и удвоения точек эллиптической кривой. Например, точка 25*P* может быть представлена, как 25*P* = 2(2(2(2*P*)) + 2(2(2*P*))) + *P*.

Понятно, что каждая точка на плоскости задается парой координат: *х* и *у*.

Числа х и у являются рациональными, а точки *P*, *Q*, *R* и -*R* (как и любые точки ЭК) – рациональными точками

**ЭК над конечными полями**

Именно этот тип ЭК будет нас интересовать в плане практического применения.

**Определение 6.** Конечное поле – это множество конечного числа элемен- тов. Примером конечного поля является множество целых чисел по модулю *p*, где *p* – простое число.

Поле обозначается как *GF*(*p*) или *Fp*. Здесь операции сложения и умножения работают как в модулярной арифметике.

Например, поле *F13* (*р* = 13) состоит из чисел: 0, 1, … , 12.

**Определение 7.** Эллиптическая кривая над полем *Fp* задается теми же уравнениями, что и ЭК над действительными числами, только все вычисления производятся по модулю *р* (mod *p*),

Формально ЭК над полем задается так: *Ер*(*а*, *b*).

Важно отметить, что, как и ранее, существует точка (бесконечно удален- ная) *О*; *а* и *b* – вещественные числа.

Прежде, чем приступить к алгебраическим операциям над точками кри- вой, такими как суммирование двух разных точек на ЭК и удвоение точек, кратко проанализируем операции для расчета точек, принадлежащих ЭК. Должны быть приняты некоторые предположения, такие как площадь, на ко- торой будут рассчитываться точки кривой, и функция кривой.

**Определение 8.** Если мы складываем два значения, кратных *Р*, то получаем значение, кратное *Р* (т.е. значения, кратные *Р*, замкнуты относительно операции сложения). Это означает, что множество кратных *Р* значений – это циклическая подгруппа группы, образованной эллиптической кривой.

**Определение 9.** Наименьшее значение числа *q*, для которого выполняется равенство *qР* = *О*, называется порядком точки *Р*.

**Определение 10.** Порядок группы точек эллиптической кривой равен числу различных точек ЭК, включая точку *О*.

**Определение 11.** Точка *Р* называется генератором или базовой точкой циклической подгруппы (такую точку во многих документах обозначают символом *G*).

Порядок точки *Р* связан с порядком *m* ЭК теоремой Лагранжа, согласно которой порядок подгруппы – это делитель порядка исходной группы. Иными словами, если ЭК содержит m точек, а одна из подгрупп содержит *q*, то *q* является делителем *m*.

Для ЭК *Ер*(*а*, *b*) порядок m группы точек должен удовлетворять неравен- ству:

Как и в случае с непрерывными ЭК, теперь важным является вычисление некоторого числа *d*, если мы знаем *P* и *Q* для *Q* = *dP*. Это и есть задача дискретного логарифмирования для эллиптических кривых.

Эта задача аналогична задаче дискретного логарифмирования, используемой в других криптосистемах, таких как алгоритм *DSA*, протокол Диффи- Хеллмана и схема Эль-Гамаля.

В криптографии на основе ЭК тайный ключ – это случайное целое *d*, выбранное из множества {1, 2, ..., *q*–1}, где *q* – порядок подгруппы; открытый ключ – это точка *Q*, такая, что *Q* = *dG*, где *G* – базовая точка подгруппы.

Криптостойкость алгоритмов на основе ЭК определяется, например, для алгоритма ЭЦП в стандарте РБ параметром l, называемым уровнем стойкости и принимающим значения (рекомендуется) из {128, 192, 256}. При этом для взлома ключа злоумышленнику нужно выполнить 2l операций.

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

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

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.

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

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

**Определение 1.** Эллиптические кривые – математический объект, который может быть определен над любым полем.

**Определение 2**. Эллиптическая кривая над вещественными числами – это множество точек, описываемых уравнением

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.

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 строна.

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*).

Поскольку символы *а* и *b* мы зарезервировали в текущей работе для обо- значения 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*.

**Практическая часть**

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

**Вывод**

В данной лабораторной работе я закрепила теоретические знания по ЭЦП. А также, разработала приложение для генерации и верификации по 3 алгоритмам.

На рисунке приведен общий интерфейс программы.

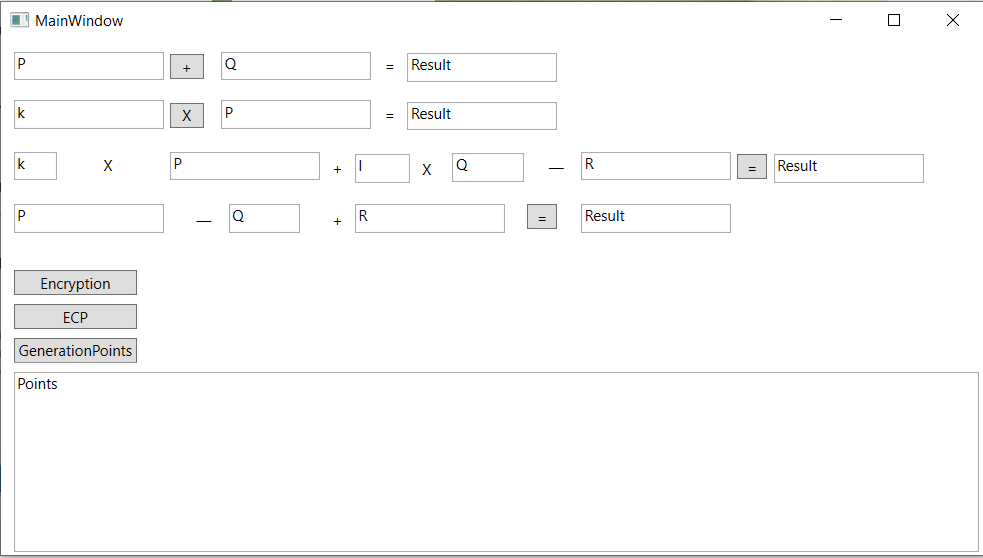
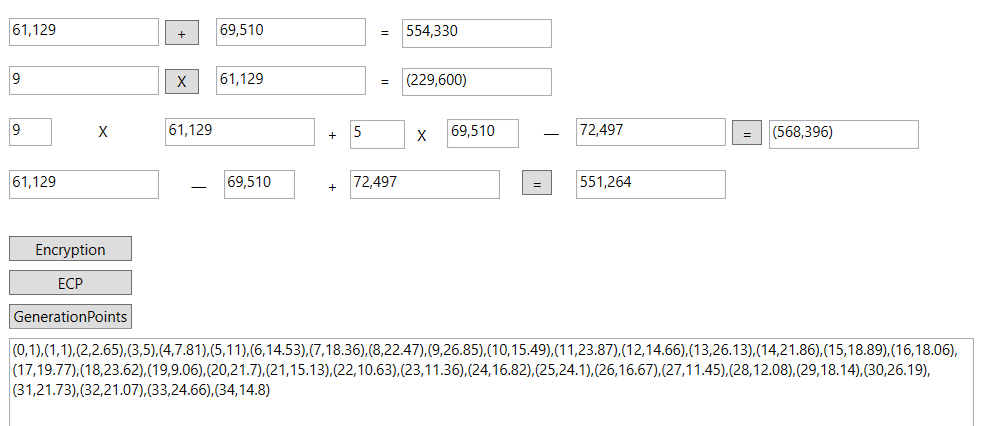


Рисунок 2.1 – Общий интерфейс программы

Далее приведен скриншот выполнения 1 и 2 заданий согласно варианту №13



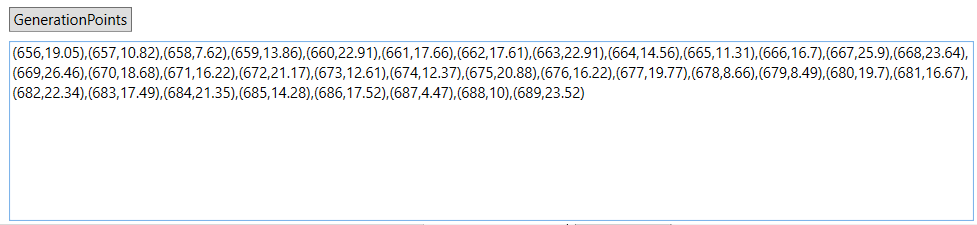


Рисунок 2.2 – Вычисление значений

Далее приведен скриншот выполнения задания №3 и шифрование расшифрование своей фамилии.

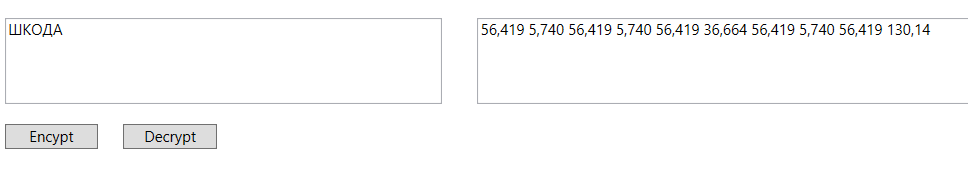


Рисунок 2.3 – Шифрование/Дешифрование Фамилии на основе ЭК

В следующем задании необходимо было реализовать генерацию и верификацию ЭЦП на основе алгоритма ECDSA. Вычислить самостоятельно значение открытого ключа, *Q*. ЭК *Е*751(–1, 1) c генерирующей точкой   
*G* = (416, 55); порядок точки *q* = 13. Тайный ключ равен 44. В итоге имеем приложение, которое отображает получившийся открытые ключ и выводит булевское значение, отражающее подлинность ЭЦП

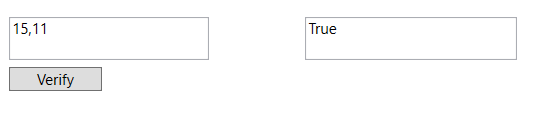


Рисунок 2.4 – ЭЦП

**Анализ результатов**

Анализ результатов показал, что заняло всего 57.23 микросекунды. Это свидетельствует о том, что шифрование было выполнено очень быстро. Такое низкое время выполнения может быть полезным в приложениях, где требуется обработка большого объема данных или быстрый отклик системы.

В целом, низкое время выполнения шифрования является позитивным показателем, что говорит о эффективности алгоритма и хорошей производительности системы.

**Вывод**: в результате лабораторной работы была изучена теория по Эллиптическим кривым, а также основная информация по методам нахождения и вычисления. Также была разработана программа, реализующая требуемые в условии задания