МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №11-2**

**″Исследование криптографических алгоритмов на основе эллиптических кривых″**

Выполнила:

Студентка 3 курса 5 группы Бобрик В.С.

Проверила: Копыток Д.В.

Минск 2021

**Цель**: изучение и приобретение практических навыков разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых.

**Задачи**:

* Закрепить теоретические знания по алгебраическому описанию и геометрическому представлению операций над эллиптическими кривыми (ЭК): по алгоритмам согласования ключевой информации на основе ЭК, алгоритмам зашифрования/расшифрования информации на основе асимметричной криптографии и ЭК, алгоритмам генерации и верификации электронной цифровой подписи на основе асимметричной криптографии и ЭК, оценке криптостойкости систем на основе ЭК.
* Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для потокового зашифрования/расшифрования.
* Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК.
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теория.** Реализация алгоритма зашифрования/расшифрования на основе ЭК. Рассмотрим это на примере алгоритма Эль-Гамаля. Вспомним, что зашифрованное сообщение М или каждый зашифрованный блок (mi) этого сообщения состоят из двух чисел. Блок шифротекста 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 шифротекст – 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.

Получатель для расшифрования сообщения вычисляет: P = С2 – dC1.

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

**Задание.** Во втором задании данной лабораторной работы необходимо было разработать приложение для зашифрования/расшифрования собственной фамилии на основе ЭК, указанной в первой части данной лабораторной работы, для генерирующей точки G = (0, 1). Тайный ключ – в соответствии с вариантом. Для варианта 1 d = 41.

Функция, выполняющая шифрование на основе ЭК представлена на рисунке 1.

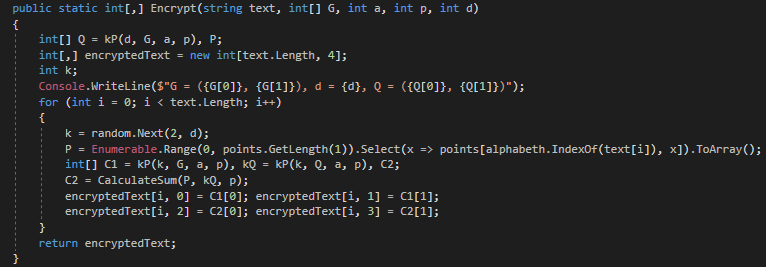


Рис. 1 – Функция для шифрования на основе ЭК

Функция, выполняющая расшифрование на основе ЭК представлена на рисунке 2.

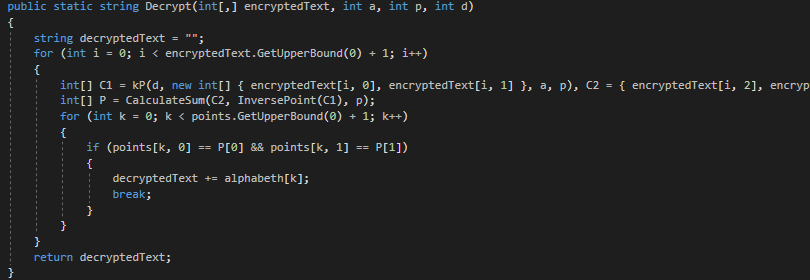


Рис. 2 – Функция для расшифрования на основе ЭК

Результаты работы приложения представлены ниже рисунке 3.

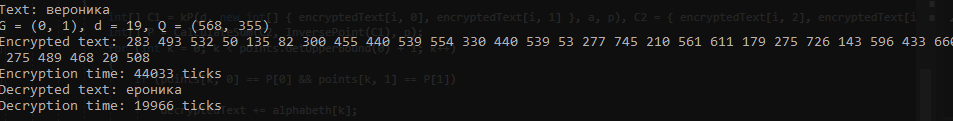


Рис. 3 – Результаты работы приложения

Вывод: в результате данной лабораторной работы было разработано приложение для зашифрования/расшифрования на основе ЭК.