МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

Кафедра информационных систем и технологий

**«Исследование криптографических алгоритмов на основе эллиптических кривых. Задание №2.»**

Студент:

Септилко Анастасия Антоновна

Преподаватель:

Блинова Евгения Александровна

Минск 2020

**ЗАДАНИЕ №2:**

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.



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 = g^k mod p, bi = (y^k•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.

В данной части лабораторной работы было необходимо создать приложение, реализующие зашифрование и расшифрование текста на основе ЭК. Обработчик на кнопку зашифрования приведена ниже на рисунке 1.1.

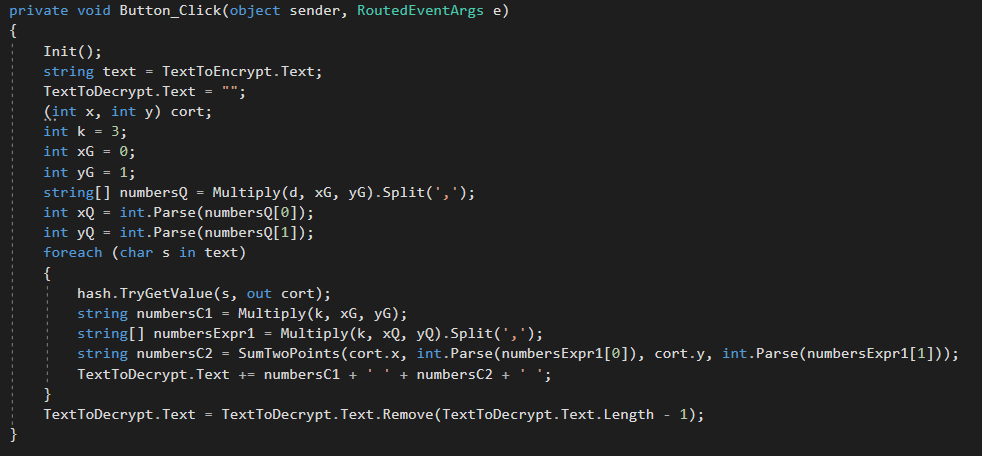


Рисунок 1.1 – Зашифрование

Обработчик на кнопку расшифрования приведена ниже на рисунке 1.2.

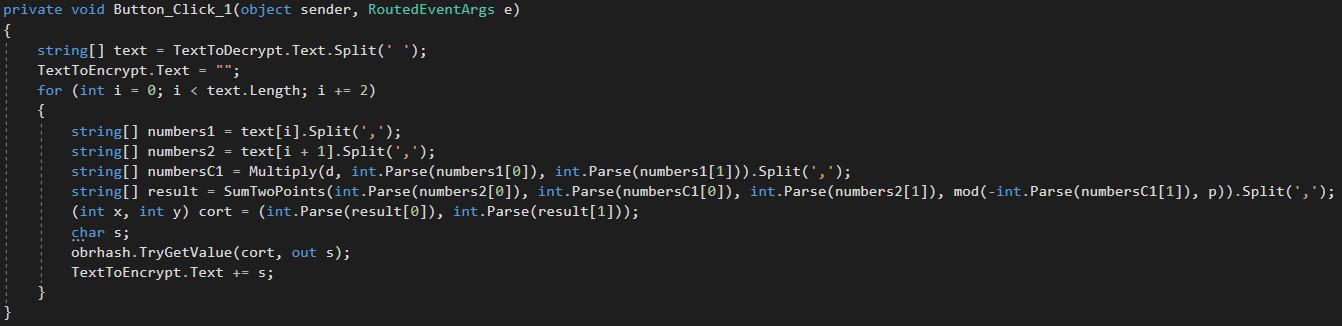
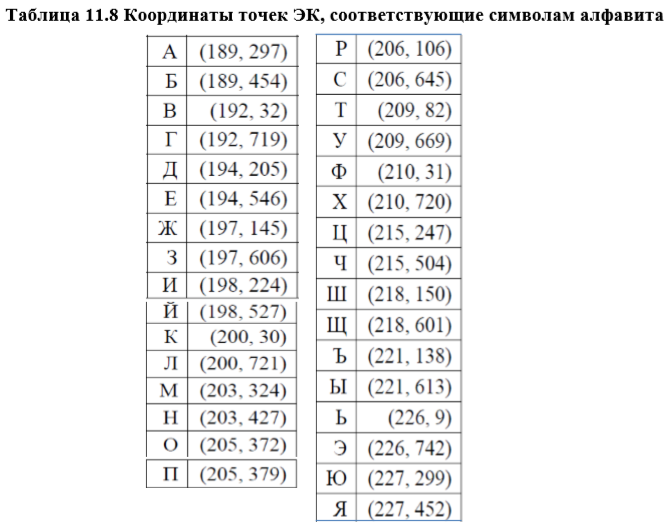


Рисунок 1.2 – Расшифрование

Для зашифрования было выбрано мое имя «Настя». Координаты точек эллиптических кривых были выбраны в соответствии с таблицей 1.8 методического пособия.



В программе за это отвечает функция Init(), которая продемонстрирована на рисунке 1.3.

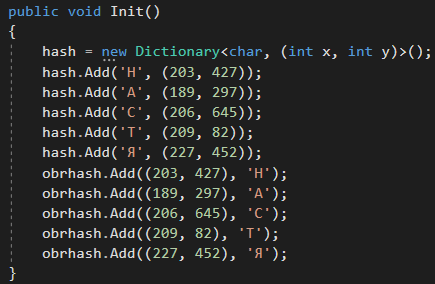


Рисунок 1.3 – Функция Init()

Исходя из теоретической части для зашифрования и расшифрования собственного имени было необходимо разработать функцию, которая отвечает за сумму двух точек. Функция SumTwoPoints() отвечает за это действие, пример ее продемонстрирован в листинге 1.1.

Листинг 1.1 – Функция SumTwoPoints()

string SumTwoPoints(int xP, int xQ, int yP, int yQ)

{

BigInteger lyambda;

int raznX = xQ - xP;

int raznY = yQ - yP;

if (raznX < 0)

{

raznX += p;

}

if (raznY < 0)

{raznY += p;}

if (xP == 0 & yP == 0)

{

return xQ.ToString() + ',' + yQ;

}

if (xQ == 0 & yQ == 0)

{

return xP.ToString() + ',' + yP;

}

BigInteger xR = 0, yR = 0;

if (xP == xQ && yP != yQ || (yP == 0 && yQ == 0 && xP == xQ))

{ }

else

{

if (xP == xQ && yP == yQ)

{

lyambda = (3 \* BigInteger.Pow(xP, 2) - 1) \* (Foo(2 \* yP, p));

}

else

{

lyambda = (raznY) \* Foo(raznX, p);

}

xR = (BigInteger.Pow(lyambda, 2) - xP - xQ);

yR = yP + lyambda \* (xR - xP);

xR = xR % p < 0 ? (xR % p) + p : xR % p;

yR = -yR % p < 0 ? (-yR % p) + p : (-yR % p);

}

string Result = xR.ToString() + ',' + yR.ToString();

return Result;

}

Итог выполнения программы показан на рисунке 1.4.



Рисунок 1.4 – Итог выполнения программы

**Вывод**

В данной части лабораторной работы был изучен способ использования эллиптических кривых в криптографии для генерации ключевой информации, рассмотрены способы использования этой информации в различных алгоритмах и создано приложение, реализующие зашифрование и расшифрование текста с использованием ЭК и алгоритма Эль-Гамаля.