МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Отчет по лабораторной работе №13-3**

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

Выполнила студентка 3 курса 5 группы Максимчикова Ю. С.

Проверила: Блинова Е. А.

Минск 2020

**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.

**Задание.** В третьем задании данной лабораторной работы необходимо было разработать 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. Для варианта 11 d = 12.

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

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 В отсылаются сообщение М и ЭЦП (числа r и s).

Функция, выполняющая генерацию ЭЦП на основе алгоритма ЕСDSA представлена на рисунке 1.

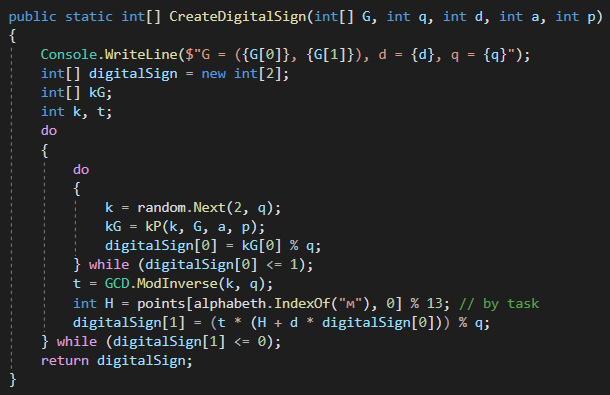


Рис. 1 – Функция для генерации ЭЦП на основе алгоритма ЕСDSA

Краткая характеристика алгоритма верификации ЭЦП. Получатель знает алгоритм хеширования, который использовался отправителем, открытый ключ отправителя, с помощью чего выполняет следующие операции над М и полученной ЭЦП.

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.

Функция, выполняющая верификацию ЭЦП на основе алгоритма ЕСDSA представлена на рисунке 2.

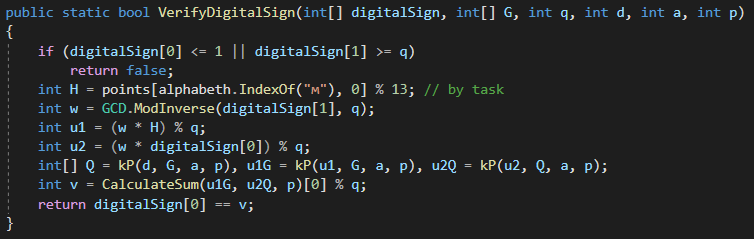


Рис. 2 – Функция для верификации ЭЦП на основе алгоритма ЕСDSA

Результаты работы приложения представлены ниже рисунке 3.

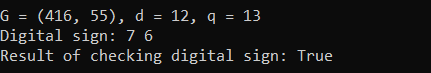


Рис. 3 – Результаты работы приложения

Вывод: в результате данной лабораторной работы было разработано приложение для генерации/верификации ЭЦП на основе алгоритма ЕСDSA.