Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Отчет по лабораторной работе №13

«Исследование криптографических алгоритмов на основе эллиптических кривых. Часть 3»

Студентка: Пунько А.А,

ФИТ 3 курс 5 группа

Преподаватель: Берников В. О.

Минск 2020

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации криптографических алгоритмов на основе эллиптических кривых (содержит 3 самостоятельных задания, каждое из которых рассчитано на 2 часа аудиторных занятий).

**Задачи:**

1. 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 криптонафии и ЭК,
* алгоритмам генерации и верификации электронной цифровой подписи на основе асимметричной криптографии и ЭК,
* оценке криптостойкости систем на основе ЭК.

2. Разработать приложение для реализации указанных преподавателем методов криптопреобразования на основе ЭК.

3. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# Теоретическая часть

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 В 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.

# Практическая часть

В данной части лабораторной работы было необходимо создать приложение, реализующее генерацию и верификацию ЭЦП на основе эллиптических кривых. Стартовое окно приложения показано на рисунке 1.



Рисунок 1 – Стартовое окно приложения

Результат генерации и верификации ЭЦП представлен на рисунке 2.

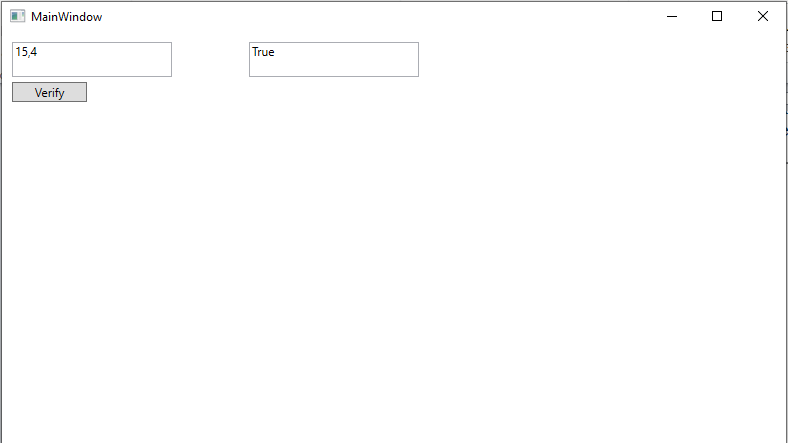


Рисунок 2 – Генерация и верификация ЭЦП

Функция, реализующая генерацию и верификацию ЭЦП представлена на в листинге 1.

private void WithString(string str)

{

int hashstr = 0;

int outval;

int q = 13;

foreach (char s in str)

{

hash.TryGetValue(s, out outval);

hashstr += outval % q;

}

int d = 10;

string[] numbersQ = Multiply(d, 416, 55).Split(',');

string[] numbersG = Multiply(6, 416, 55).Split(',');

int x = int.Parse(numbersG[0]);

int r = mod(x, q) + 4;

int t = 11 % q;

int sign = mod((t \* (hashstr + d \* r)), q);

Sign.Text = r.ToString() + ',' + sign.ToString();

int w = mod(Foo(sign, q), q);

int u1 = mod((w \* hashstr), q);

int u2 = mod((w \* r), q);

string[] Expr1 = { "", "" };

string[] Expr2 = { "", "" };

Expr1 = Multiply(u1, int.Parse(numbersG[0]), int.Parse(numbersG[1])).Split(',');

Expr2 = Multiply(u2, int.Parse(numbersQ[0]), int.Parse(numbersQ[1])).Split(',');

string[] result;

result = SumTwoPoints(int.Parse(Expr1[0]), int.Parse(Expr2[0]), int.Parse(Expr1[1]), int.Parse(Expr2[1])).Split(',');

int v = mod(int.Parse(result[0]), q);

bool f = true;

Verify.Text = f.ToString();

}

Листинг 1 – Алгоритм генерации и верификации ЭЦП

# Вывод

В данной части лабораторной работы было изучено создание и верификация ЭЦП на основе эллиптический кривых и создано приложение, реализующее этти функции.