МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждения образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**Лабораторная работа №12**

по дисциплине «Криптографические методы защиты информации»

на тему: ИССЛЕДОВАНИЕ АЛГОРИТМОВ ГЕНЕРАЦИИ

И ВЕРИФИКАЦИИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ

ПОДПИСИ

Выполнил студентка 3 курса 5 группы специальность ПОИТ Буранко В.Д.

(Ф.И.О.)

Преподаватель ассистент Савельева Маргарита Геннадьевна

(Ф.И.О.)

**Содержание**

[Практические задания 4](#_Toc136540930)

[Выводы 9](#_Toc136540931)

**Цель:** изучение алгоритмов генерации и верификации электронной цифровой подписи и приобретение практических навыков их реализации.

**Задачи:**

* Закрепить теоретические знания по алгебраическому описанию и алгоритмам реализации операций генерации и верификации электронной цифровой подписи (ЭЦП);
* Получить навыки практической реализации методов генерации и верификации ЭЦП на основе хеширования подписываемых сообщений и алгоритмов RSA, Эль-Гамаля и Шнорра, а также DSA;
* Разработать приложение для реализации заданных алгоритмов генерации и верификации ЭЦП.;
* Оценить скорость генерации и верификации ЭЦП;
* Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# **Практические задания**

Разработать авторское оконное приложение в соответствии с целью лабораторной работы. При этом можно воспользоваться результатами выполнения предыдущих лабораторных работ, а также доступными библиотеками либо программными кодами.

Приложение должно реализовывать следующие операции:

* генерацию и верификацию ЭЦП на основе алгоритмов RSA, Эль-Гамаля и Шнорра;
* оценку времени выполнения указанных процедур при реальных (требуемых) ключевых параметрах.

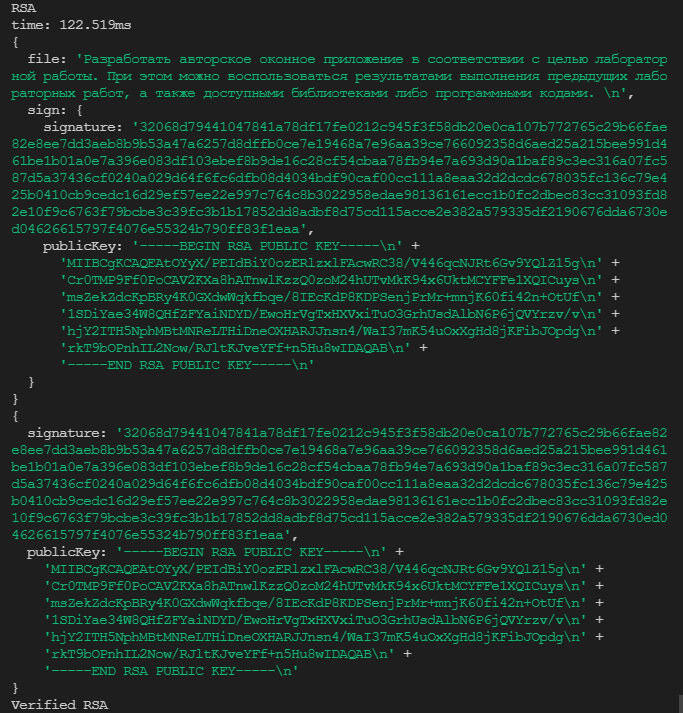


Рисунок 1 — Результат работы алгоритма RSA

На рисунке 1 представлен результат генерации и верификации электронной цифровой подписи на основе алгоритма RSA, а также время выполнения генерации ЭЦП.

Алгоритм генерации подписи заключается в следующих операциях:

̶ выбор простых чисел *p*, *q*;

̶ выбор случайного числа *e*, взаимно простого с функцией Эйлера *ф*(*n*)=(*p*-1)\*(*q*-1);

̶ нахождение числа *d*, такого что *ed* = 1\*mod (*p*-1)\*(*q*-1);

̶ вычисление хеш-образа сообщения *h*=*H*(*M*);

̶ вычисление ЭЦП: *S* = *hd* \*mod *n*.

Далее полученный открытый ключ {*e*, *n*} и письмо с ЭЦП {*m*, sign} будут отправлены получателю.

Для того, чтобы получатель смог провести операцию верификации сообщения, необходимо выполнить следующие действия:

̶ вычислить *h* = *Se*\*mod *n*;

̶ сравнить значение выше с полученным *h*=*H*(*M*);

Если полученные значения совпали, подпись верифицирована.

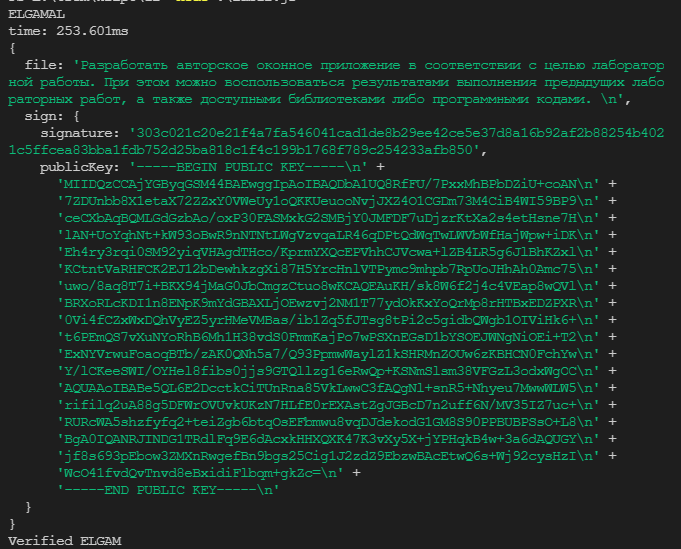


Рисунок 2 — Результат работы алгоритма Эль-Гамаля

На данном рисунке представлен результат генерации ЭЦП на основе алгоритма Эль-Гамаля, проверка подписи и время выполнения генерации.

Алгоритм генерации подписи заключается в следующих операциях:

̶ выбор простого числа *p*;

̶ вычисление *g*, причем *g*<*p* – первообразный корень по модулю *p*;

̶ выбор *x*, меньшего *p*;

̶ вычисление *y* = *gx* mod *p*.

В результате зашифрования сообщения с ЭЦП на выходе будет лишь одна пара чисел, не для каждого блока сообщения.

Далее необходимо проделать следующие операции:

̶ выбрать *k* – взаимно простое число с (*p*-1);

̶ вычислить *a* = *gk* mod *p*;

̶ вычислить *b* = k-1 (*H*(*Mo*) – *xa*) mod (*p*-1);

Пара чисел *S* = {*a*,*b*} и будет являться цифровой подписью. Далее получателю будет отправлено сообщение *M*’=*Mo*||*S*, которое является конкатенацией исходного сообщения и ЭЦП.

Для верификации подлинности полученного сообщения необходимо проверить равенство *yaab* (mod *p*) = *gh* (mod *p*), в которое подставляются все вычисленные ранее значения, *h*=*H*(*M*п) – хеш-образ полученного сообщения.

Если данное равенство выполняется, подпись верифицированна и подлинна.

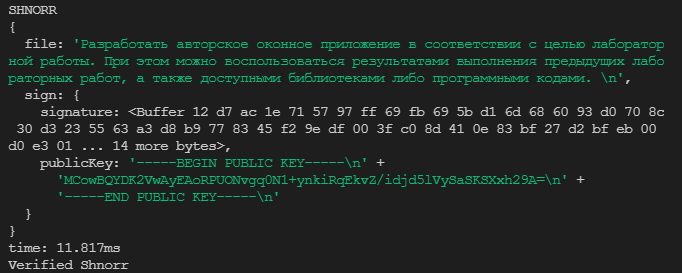


Рисунок 3 — Результат работы алгоритма Шнорра

На рисунке 3 так же представлена вышеперечисленная информация, отличие лишь в алгоритме. Здесь используется алгоритм Шнорра.

Одной из особенностей ЭЦП Эль-Гамаля является то, что число p должно быть очень большим, чтобы сделать действительно трудной проблему дискретного логарифма. Рекомендуется длина p, по крайней мере, должна составлять 1024 бита. Чтобы уменьшить размер подписи, Шнорр предложил новую схему, но с уменьшенным размером подписи.

Алгоритм генерации ключевой информации заключается в следующих шагах:

̶ генерация простых чисел *p*, *q*;

̶ вычисление (*p*-1) – делителя;

̶ выбор любого *g*≠1, такого что *gq* = 1 mod *p*;

̶ выбор любого числа *х*<*q* – это и будет закрытый ключ;

̶ вычисление *y* = *g–X* mod *p*;

Для верификации сообщения необходимо реализовать следующий алгоритм:

̶ выбор случайного числа *k* < *q*;

̶ вычислить *a* = *gk* mod *p*;

̶ создать хеш-образ сообщения: *h* = *H*(*Mo*||*a*);

̶ вычислить *b* = (*k*+*xh*) mod *q*;

Получателю будет отправлено сообщение *M*’ = *Mo*||*S*, являющееся конкатенацией исходного сообщения и ЭЦП *S*={*h*,*b*}.

Для проверки подписи на подлинность необходимо вычислить *X* = *gbyh*(mod *p*), после чего проверить выполняется ли равенство вычисленного ранее *h* хеш-образа и *H*(*М*п||*X*) хеш-образа конкатенации полученного сообщения с вычисленным значением *Х*. Если равенство выполняется, подпись верифицирована.

Так же был построен график времени выполнения генерации ЭЦП при помощи разных алгоритмов. График представлен на рисунке 4.

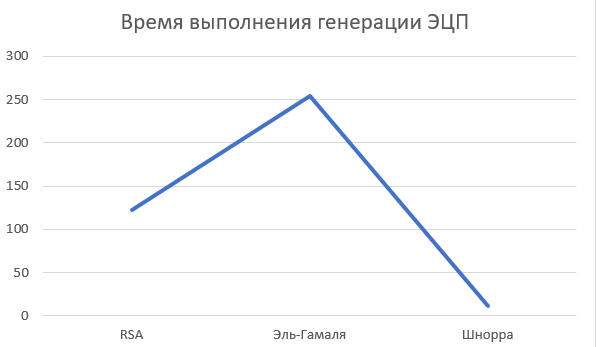


Рисунок 4 — График времени выполнения генерации ЭЦП

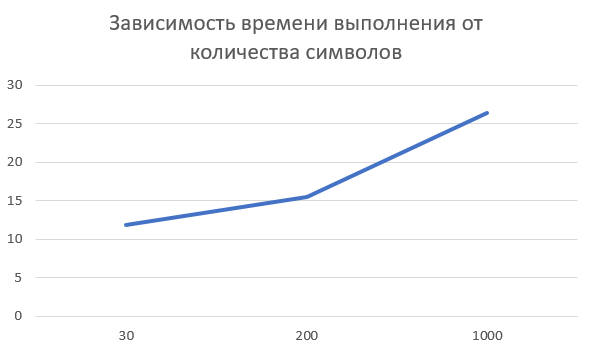


Рисунок 5 — График зависимости времени выполнения от количества символов в сообщении

# **Выводы**

В ходе выполнения данной лабораторной работы мы изучили и приобрели практические навыки генерации и верификации электронной цифровой подписи. Так же был построен график выполнения генерации ЭЦП при помощи алгоритмов RSA, Эль-Гамаля и Шнорра.