Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Исследование криптографических алгоритмов на основе эллиптических кривых

Студент: Валдайцев А. Д.

ФИТ 3 курс 5 группа

Пр*еп*одаватель: Савельева М. Г.

Минск 2023

# Алгоритм RSA

При генерации ЭЦП с использованием алгоритма RSA можно рассматривать две ситуации:

* сообщение *Мо* подписывается и передается в открытом (незашифрованном) виде;
* сообщение *Мо* подписывается и передается в зашифрованном виде.

Первый случай соответствует ситуации, когда этом подпись *S* вычисляется на основе соотношения



при указанном выше реверсе в отношении ключевой информации; *dо* и *nо* – элементы тайного ключа отправителя.

Передаваемое сообщение *М’* = *Мо*|| *S*. Соответственно, операция расшифрования на приемной стороне (получатель анализирует *Мп*|| *S*) будет производиться в соответствии с формулой с известной модификацией ключей:



Далее вычисляется *Н*(*Mп*). Если *H*(*Mo*) = *H*(*Mп*), подпись верифицирована. Если подписываемое сообщение *М*(*М’*) также должно передаваться в зашифрованном виде, то обычно *М’* шифруется на стороне отправителя стандартным образом: с помощью открытого ключа получателя (*еп* и *nп*), который перед основным процессом верификации подписи расшифровывает послание своим тайным ключом: *dп* и *nп*. Далее осуществляются вычисления и анализ, как и в первом случае.

Код функции для генерации и верификации ЭЦП на основе алгоритма RSA представлен на рисунке 1.1.



Рисунок 1.1 – Код функции генерации и верификации ЭЦП на основе алгоритма RSA

# Алгоритм Эль-Гамаля

Ключевая информация отправителя: открытый ключ: *y*, *g* и *р*; тайный ключ: *х*. Чтобы подписать сообщение *Мо*, обладатель используемых для ЭЦП ключей должен выбрать случайное число *k*, взаимно простое с (*р* – 1). Затем вычисляются числа *а* и *b*, являющиеся цифровой подписью (*S* = {*a*, *b*}).

Для вычисления параметра *b* с помощью расширенного алгоритма Евклида решается следующее уравнение:



Получателю отправляется сообщение *М’* = *Мо*|| *S*. Для верификации подписи вычисляется хеш полученного сообщения *Н*(*Мп*) = *h*. Далее нужно убедиться, что выполняется равенство



Если равенство выполняется, подпись верифицируется.

Код функции для генерации и верификации ЭЦП на основе алгоритма Эль-Гамаля представлен на рисунке 2.1.

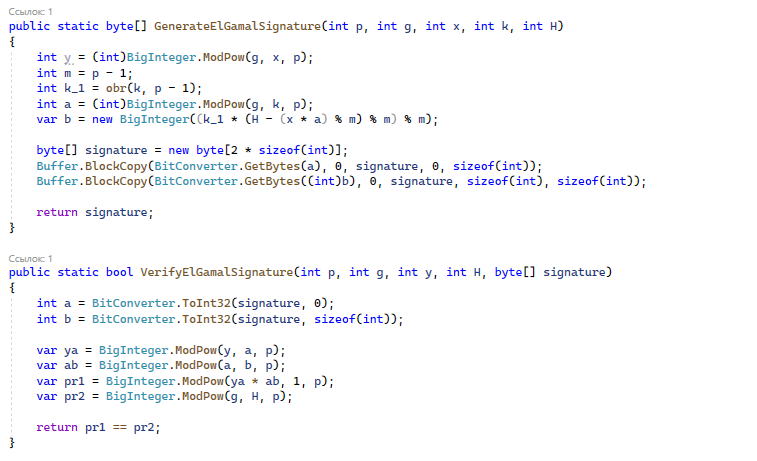


Рисунок 2.1 – Код функции генерации и верификации ЭЦП на основе алгоритма Эль-Гамаля

# Алгоритм Шнорра

Алгоритм Шнорра является вариантом алгоритма ЭЦП Эль-Гамаля.

Числа *p*, *g*, *q* являются открытыми и могут применяться группой пользователей. Выбирается число *х* < *q* (*х* является тайным ключом) и вычисляется последний элемент открытого ключа:



Секретный ключ имеет длину не менее 160 битов. Для подписи сообщения *Мо* выбирается случайное число *k* (1 < *k* < *q*) и вычисляется параметр *а*.



Получателю отправляются *М’* = *Мо* || *S*; *S* = {*h*, *b*}. Для проверки подписи получатель вычисляет



Затем он проверяет выполнение равенства: *h* = *Н*(*Mп* || *Х*). Подпись достоверна, если равенство выполняется.

Код функции для генерации и верификации ЭЦП на основе алгоритма Шнорра представлен на рисунке 3.1.

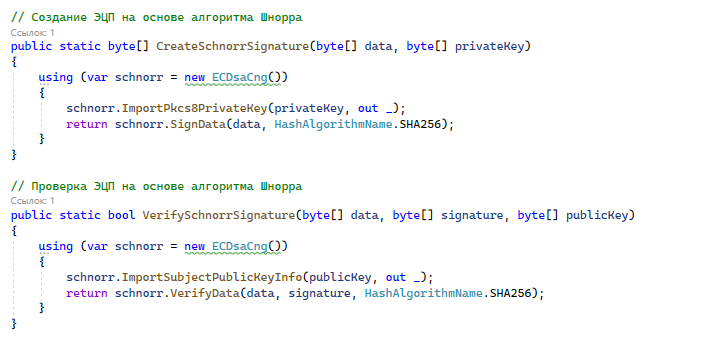


Рисунок 3.1 – Код функции генерации и верификации ЭЦП на основе алгоритма Шнорра

# Время генерации и верификации ЭЦП

Сравним время, за которое генерируется и верифицируется электронная цифровая подпись по алгоритмам RSA, Эль-Гамаля и Шнорра. График сравнения представлен на рисунке 2.1.

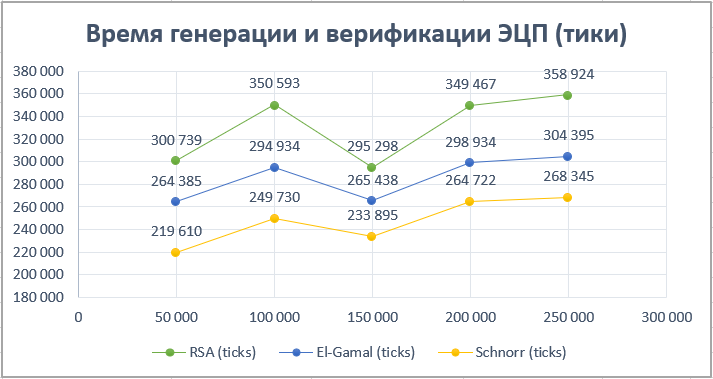


Рисунок 2.1 – Время вычисления хеша в тиках

Как видно из графика, не в зависимости от длины входного сообщения, время генерации и верификации электронной цифровой подписи всегда примерно одинаковое – примерно 300 тысяч тиков для всех алгоритмов. Однако, как видно из графиков, алгоритмы имеют немного разную скорость вычисления, и алгоритм RSA обычно занимает немного больше времени, чем алгоритм Эль-Гамаля и Шнорра, однако, данные различия являются несущественными.

# Вывод

В данный лабораторной работе были изучены алгоритмы генерации и верификации электронной цифровой подписи на основе алгоритмов RSA, Эль-Гамаля и Шнорра, а также приобретены практические навыки их реализации.