МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«Определение, назначение, основные функции и типы ЭЦП»**

Студент: Высоцкий Я.А.

ФИТ 3 курс 5 группа

Вариант 4

Преподаватель: Савельева М. Г.

Минск 2023

1. **Генерация и верификация ЭЦП на основе RSA**

Для генерации и верификации ЭЦП на основе RSA был использован ранее разработанный модуль RSA. Изначально мы генерируем закрытый и открытый ключ и хэш передаваемого сообщения. Далее мы передаем сообщение и саму подпись. Для верификации подписи, получатель вычисляет хэш сообщения и хэш подписи, а после чего сравнивает.

Код реализующий данный функционал показан ниже на рисунке 1.1

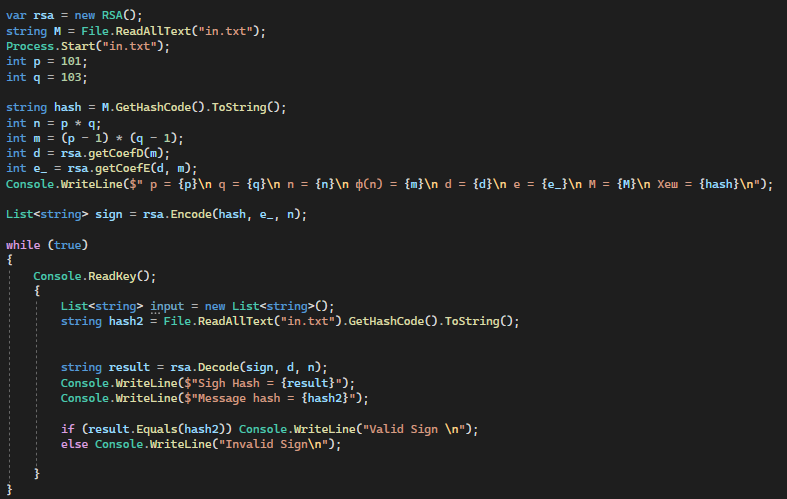
****

Рисунок 1.1 – Код генерации и валидации ЭЦП на основе RSA

Так же помимо генерации и проверки данный метод засекает время, затраченное на все процессы.

1. **Генерация и верификация ЭЦП на основе алгоритма Эль - Гамаля**

Для генерации и верификации ЭЦП на основе алгоритма Эль – Гамаля мы должны сгенерировать ключевую информацию. Нам требуется вычислить следующие коэффициенты: *y, g, p, x.* Все кроме коэффициента *x* являются открытым ключом. Затем над надо вычислить саму цифровую подпись по формуле, указанной ниже.

(2.1)

Так же требуется рассчитать коэффициент *b.*

(2.2)

А для верификации подписи вычисляется хеш полученного сообщения. Далее нужно убедиться, что выполняется следующее равенство.

(2.3)

Код реализующий описанный выше алгоритм отображен на рисунке 2.1.

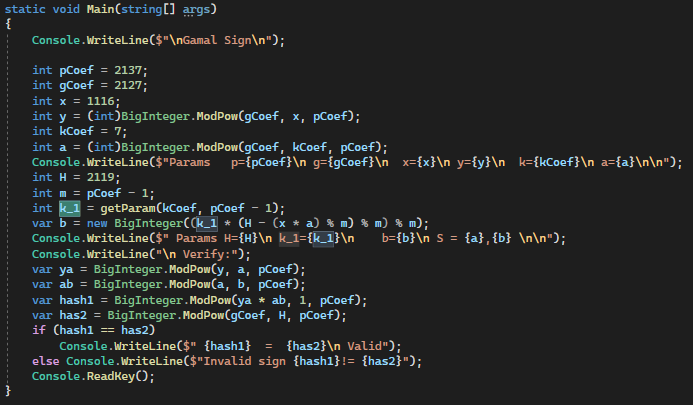
****

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

Если равенство 2.3 выполняется, то подпись верефицируется.

1. **Генерация и верификация ЭЦП на основе алгоритма Шнора**

Для генерации и верификации ЭЦП на основе алгоритма Шнора мы должны сгенерировать ключевую информацию. Нам требуется вычислить следующие коэффициенты: *p, q, g.* Коэффициент *p* – простое число в диапазоне от 512 до 1024 бит, *q* – 160-битное простое число, *g* – должен соответствовать следующему равенству.

(3.1)

Далее надо выбрать коэффициент *x<q* который является тайным ключом, для последующего вычисления последнего элемента открытого ключа – *y.*

(3.2)

Далее для подписи сообщения выбирается случайное число *k* и вычисляется число *a* по формуле (2.1). После вычисляется хэш конкатенации сообщения и числа *a* и число b.

(3.3)

Получателю для проверки подлинности вычисляет *X.*

(3.4)

Код реализующий описанный выше алгоритм отображен на рисунке 3.1.

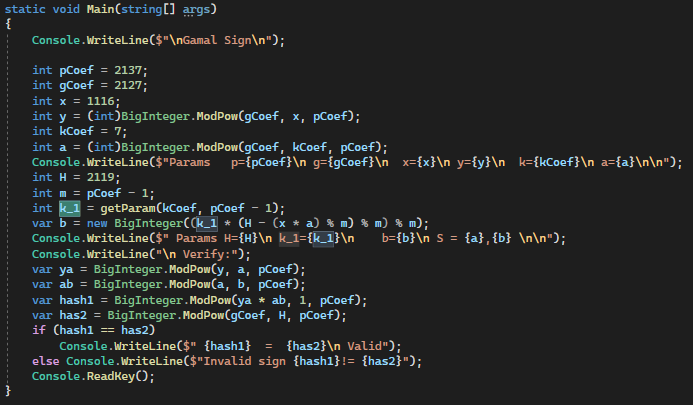
****

Рисунок 3.1 – Код генерации и валидации ЭЦП на основе алгоритма  
 Шнорра

Если хэш от конкатенации сообщения и коэфициента *X* совпадают с коэффициентом *h,*то подпись является валидной.

**4) Оценка времени выполнения**

Для оценки времени выполнения шифрования и расшифрования были взяты исходные текста с количеством символов 36, 72, 144.

Рисунок 5.1 – График времени выполненния хэширования текста алгоритмом SHA - 512

При увеличении количества символов в входном тексте время затраченное на хэширование уменьшается. Возможно это связано с накладными расходами на расширения изначального сообщения нулевыми битами.

**Вывод**

При выполнении лабораторной работы были изучены алгоритмы генерации и верификации цифровой подписи и приобретены практические навыки по их реализации.