Учреждение образования

«Белорусский Государственный Технологический Университет»

**Лабораторная работа №10**

**«**Исследование алгоритмов генерации и верификации электронной цифровой подписи»

Выполнил:

Студент 3 курса 1 группы ФИТ

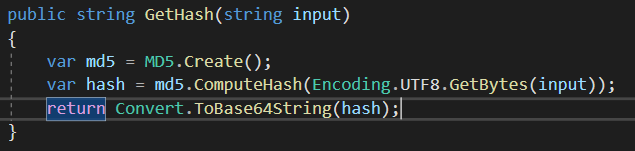
Дырда Дмитрий Геннадьевич

Минск 2020

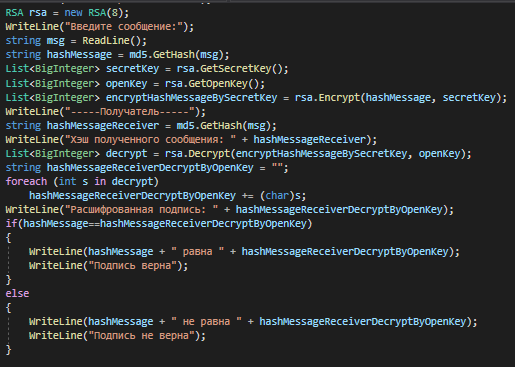
**Цель:** изучение алгоритмов генерации и верификации электронной цифровой подписи и приобретение практических навыков их реализации.

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, Шнорра;

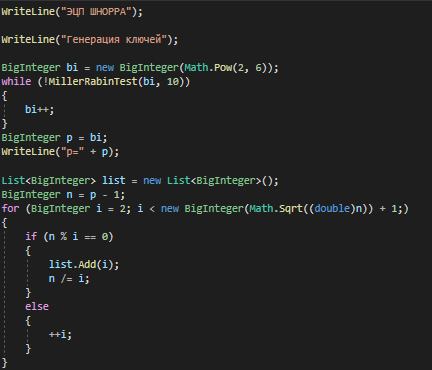
Использовался алгоритм хеширования MD5:

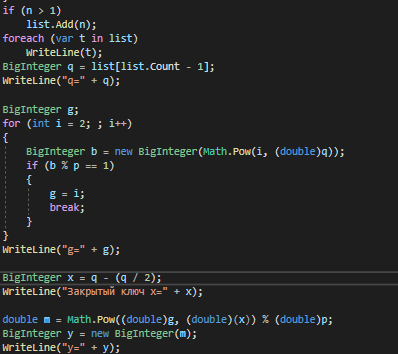


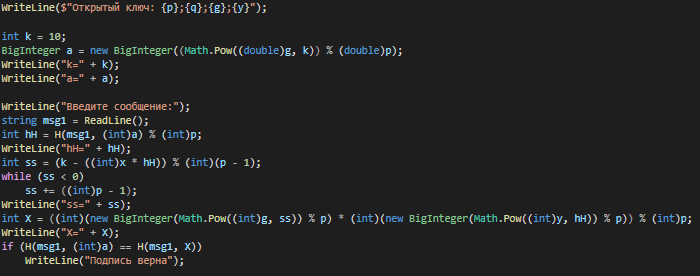
Реализация ЭЦП на основе RSA:



Реализация ЭЦП на основе Шнорра:







**Вывод:** Я изучил некоторые алгоритмы генерации и верификации электронной цифровой подписи и приобрел практические навыки их реализации.