Министерство образования Республики Беларусь

Учреждение образования

«Белорусский государственный университет пищевых и химических технологий»

Кафедра автоматизации технологических процессов и производств

**Алгоритм шифрования RSA. Цифровая подпись**

**Отчёт по практической работе №4**

Вариант 3

по дисциплине «Основы защиты информации»

Специальность 1 – 40 05 01 Информационные системы и технологии

Направление специальности 1 – 40 05 01 – 11 Информационные системы и технологии (в пищевой промышленности)

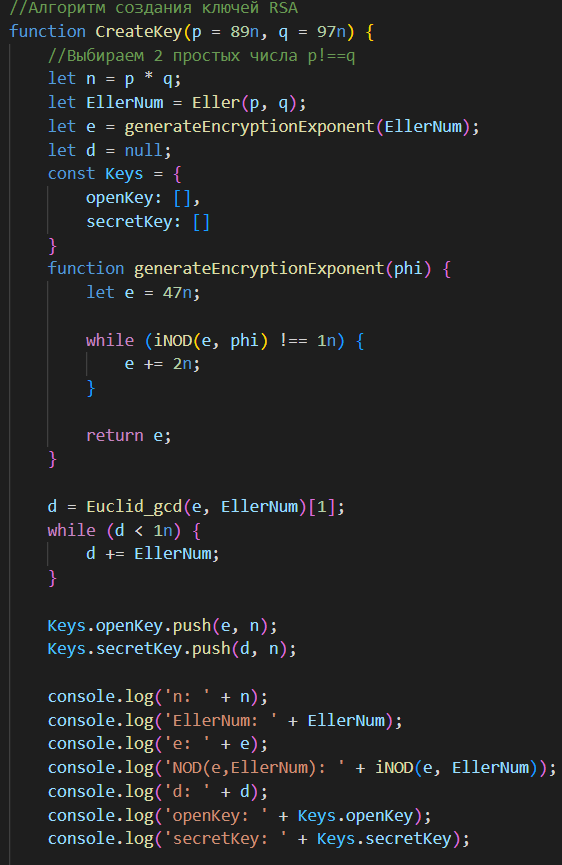
|  |  |
| --- | --- |
| Проверил  Старший преподаватель  О.Б.Ганак  «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_2023 г. | Выполнил  студент группы ИСИТ-191  О.А.Васечко  «\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_ 2023 г. |

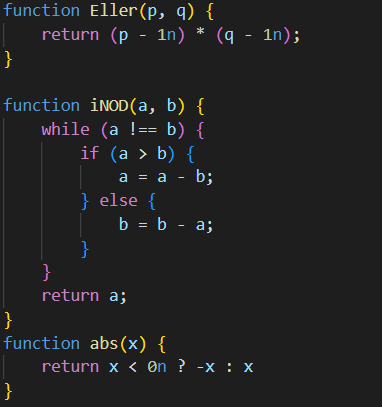
Могилев 2023

**Цель работы:** Разработать программное обеспечение, реализующее функции генерации секретного и открытого ключей, шифрования и цифровой подписи для алгоритма RSA.

**Ход работы:**

На рисунке 1 показана функция для создания ключей OpenKey и SecretKey.





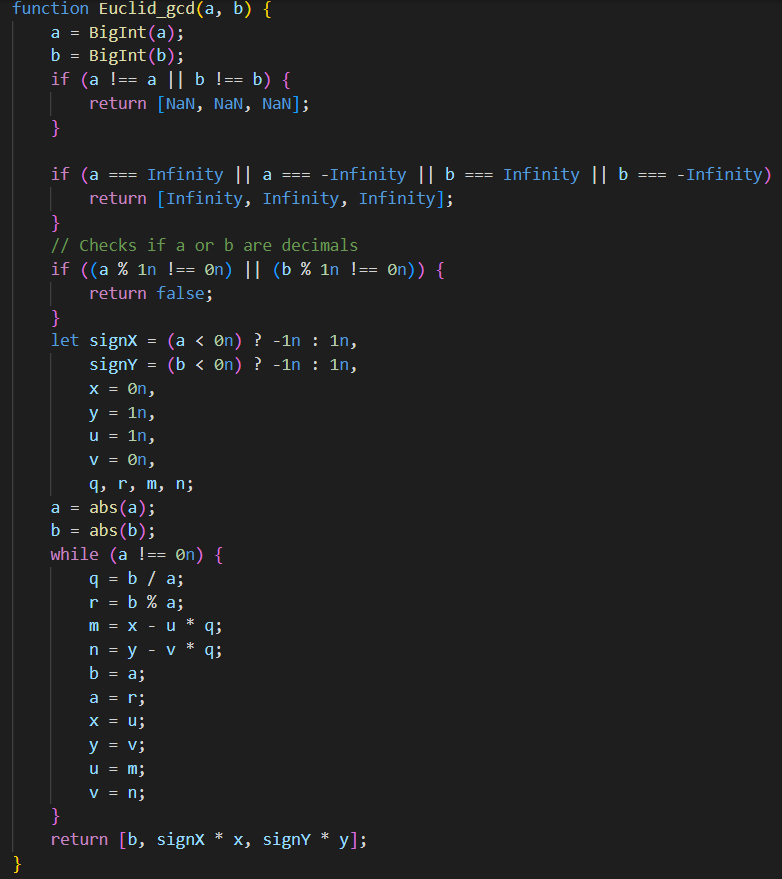


Рисунок 1 – Создание ключей

На рисунке 2 представлены функции шифрования и расшифровки сообщения m.

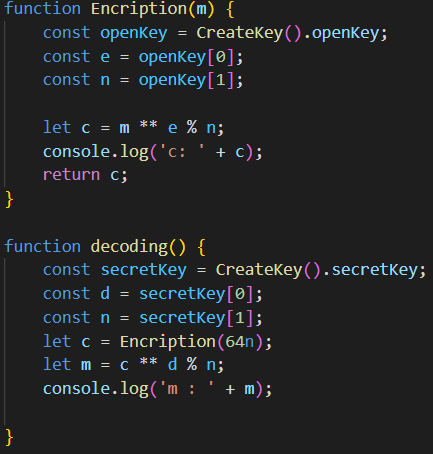


Рисунок 2 – Шифрование и расшифровка сообщения

На рисунке 3 представлены функции создания и проверки цифровой подписи



Рисунок 3 – Функции генерации и проверки цифровой подписи

На рисунке 4 представлен результат работы.

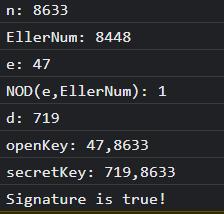


Рисунок 4 – Результат работы программы

**Вывод:** В ходе выполнения практической работы были изучены методы реализации асимметричного шифрования и электронной цифровой подписи, разработана программа реализации алгоритма RSA, а также создания и проверки электронной цифровой подписи с помощью языка программирования JavaScript.