Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет)»
(МГТУ им. Н.Э. Баумана)

ФАКУЛЬТЕТ «**Информатика и системы управления**»

КАФЕДРА «**Программное обеспечение ЭВМ и информационные технологии**»

ОТЧЁТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4

Студент Ковель Александр Денисович

Группа ИУ7-76Б

Предмет Защита информации

Студент		**Ковель А. Д.**
	подпись, дата	*фамилия, и.о.*
Преподаватель		**Чиж И. С.**
	подпись, дата	*фамилия, и.о.*

2023 г.

ВВЕДЕНИЕ

Цель лабораторной работы — разработать программу шифровальной машины «RSA» [1].

Задачи лабораторной работы:

1) провести анализ работы шифровальной машина «RSA»;
2) описать алгоритм шифрования;
3) релизовать описанный алгоритм.

1 Аналитическая часть

1.1 Алгоритм шифрования RSA

RSA [1] — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации.

Алгоритм:

— Выбираем два случайных простых числа p и q.

— Вычисляем их произведение: N = p * q.

— Вычисляем функцию Эйлера: $\varphi(N) = (p-1) * (q-1)$.

— Выбираем число e (обычно простое, но необязательно), которое меньше $\varphi(N)$ и является взаимно простым с $\varphi(N)$ (не имеющих общих делителей друг с другом, кроме 1).

— Ищем число d, обратное числу e по модулю $\varphi(N)$.Т.е. остаток от деления (d*e) и $\varphi(N)$ должен быть равен 1. Найти его можно через расширенный алгоритм Евклида.

Алгоритм шифрования RSA может использоваться в следующих режимах.

1. **MD5** — 128-битный алгоритм хеширования, разработанный профессором Рональдом Л. Ривестом из Массачусетского технологического института (Massachusetts Institute of Technology, MIT) в 1991 году. Предназначен для создания «отпечатков» или дайджестов сообщения произвольной длины и последующей проверки их подлинности. Широко применялся для проверки целостности информации и хранения хешей паролей.
2. **SHA1** — алгоритм криптографического хеширования. Для входного сообщения произвольной длины алгоритм генерирует 160-битное (20 байт) хеш-значение, называемое также дайджестом сообщения, которое обычно отображается как шестнадцатеричное число длиной в 40 цифр.

2 Конструкторская часть

2.1 Разработка алгоритма

На рисунке 1 представлена схема алгоритма шифрования RSA.

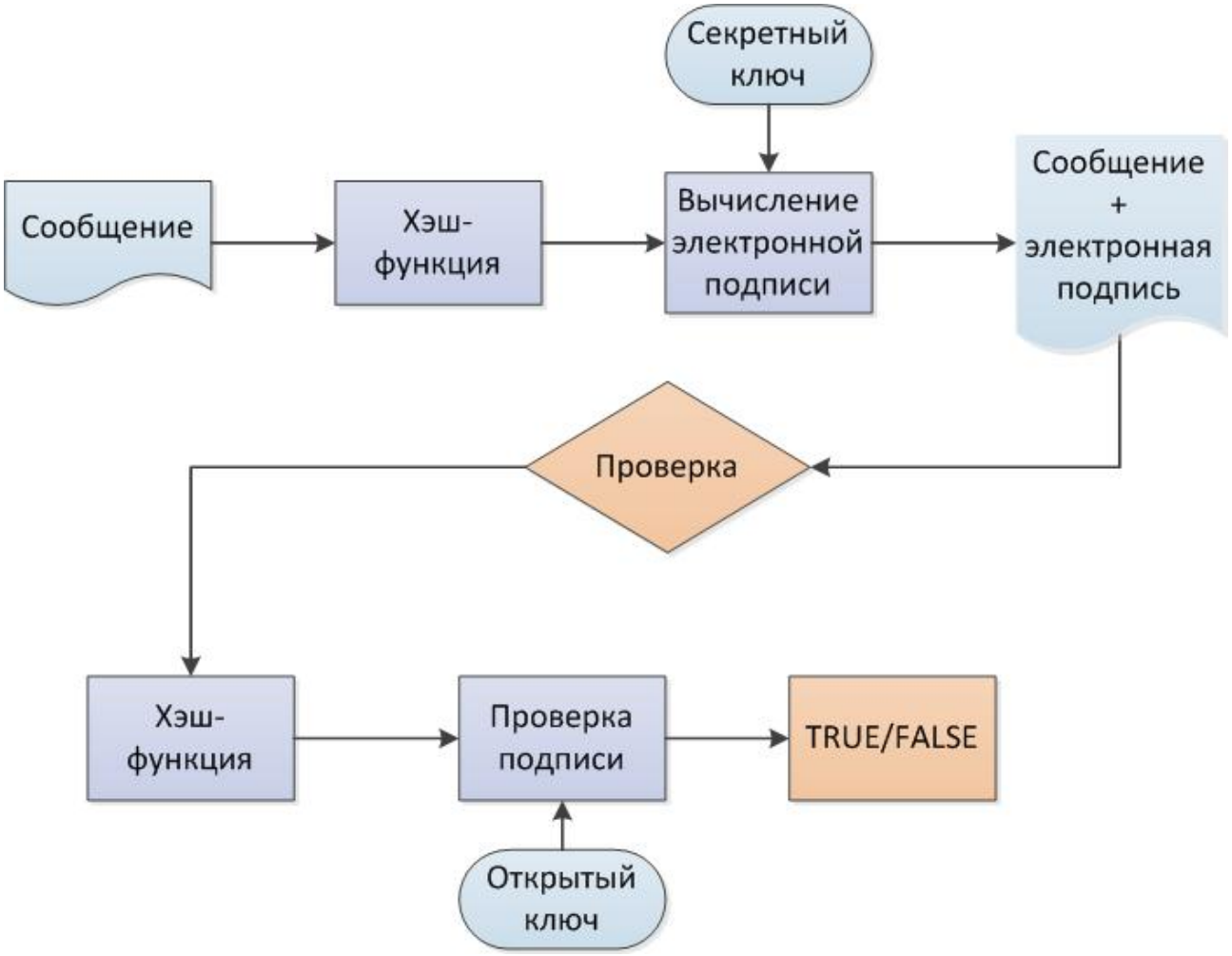

Рисунок 1 – Схемы алгоритма RSA

3 Технологическая часть

3.1 Средства реализации

Для реализации ПО был выбран язык C++ [2]. В данном языке есть все требующиеся инструменты для данной лабораторной работы. В качестве среды разработки была выбрана среда VS code [3].

3.2 Реализация алгоритма

Реализация OFB.

```
Keys calculateRSAKeys()
{
  std::vector <largeIntegerType> primes(1034);
  std::ifstream fin("input/primes.txt");
  for(int i = 0; i < 1033; i++)
  {
    int temp;
    fin >> temp;
    primes[i] = temp;
  }

  largeIntegerType p = primes[rand() % 1033];
  largeIntegerType q = primes[rand() % 1033];

  largeIntegerType n = p * q;

  largeIntegerType functionE = (p - 1) * (q - 1);

  largeIntegerType e = 1;
  for (largeIntegerType i = functionE - 1; i > 0; --i)
  {
    if (gcd(i, functionE) == 1 && prime(i))
    {
      e = i;
      break;
    }
  }

  largeIntegerType d;
  for (largeIntegerType i = 0;; ++i)
```

```
    {
      if ((largeIntegerType)i * (largeIntegerType)e %
          (largeIntegerType)functionE == 1)
      {
        d = i;
        break;
      }
    }

    Keys keys{std::pair<largeIntegerType, largeIntegerType>{e, n},
       std::pair<largeIntegerType, largeIntegerType>{d, n}};
    return keys;
  }
```

3.3 Тестовые данные

В таблице 1 приведены тесты для алгоритма шифрования RSA. Применена методология черного ящика. Тесты пройдены *успешно*.

Таблица 1 – Функциональные тесты

Входная строка	Выходная строка
$ABOBA$	$BCRGJ$
$BCRGJ$	$ABOBA$
$<<>>$	$<<>>$
A	T
T	A

ЗАКЛЮЧЕНИЕ

В данной лабораторной работе:

1) проведен анализ работы шифровальной машина «RSA»;
2) описан алгоритм шифрования;
3) реализован описанный алгоритм;

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

Список литературы

1. AES. https://e-nigma.ru/stat/rsa/. дата обращения: 17.09.2023.
2. Язык программирования C++. https://learn.microsoft.com/en-us/cpp/cpp/cpp-language-reference?view=msvc-170. дата обращения: 17.09.2023.
3. Vscode. https://code.visualstudio.com/. дата обращения: 17.09.2023.