МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
АЭРОКОСМИЧЕСКОГО ПРИБОРОСТРОЕНИЯ»

КАФЕДРА № 51

ОТЧЕТ
ЗАЩИЩЕН С ОЦЕНКОЙ

ПРЕПОДАВАТЕЛЬ

ассистент		Исаева М.Н.
должность, уч. степень, звание	подпись, дата	инициалы, фамилия

ОТЧЕТ О ЛАБОРАТОРНОЙ РАБОТЕ №4

ОДНОНАПРАВЛЕННЫЕ ХЕШ-ФУНКЦИИ

по курсу: КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

РАБОТУ ВЫПОЛНИЛ

СТУДЕНТ ГР. 5912 _____ Льдокова С.В.

подпись, дата — инициалы, фамилия

Санкт-Петербург 2022

Цель

Реализовать алгоритм хеширования ГОСТ Р 34.11-94 и провести эксперимент на «нахождение второго прообраза» и «нахождение коллизий».

1. Описание алгоритма

ГОСТ Р 34.11-94 — устаревший российский криптографический стандарт вычисления хеш-функции, основанный на ГОСТ 34.10-94. В странах СНГ переиздан и используется как межгосударственный стандарт ГОСТ 34.311-95.

Стандарт определяет алгоритм и процедуру вычисления хеш-функции для последовательности символов. Этот стандарт является обязательным для применения в качестве алгоритма хеширования в государственных организациях РФ и ряде коммерческих организаций.

До 2013 г. ЦБ РФ требовал использовать ГОСТ Р 34.11-94 для электронной подписи предоставляемых ему документов.

С 1 января 2013 года заменён РФ на ГОСТ 34.11-2012 «Стрибог», а с 1 июня 2019 года в странах СНГ на ГОСТ 34.11-2018.

Основой описываемой хеш-функции является шаговая функция хеширования $H_{out} = f(H_{in}, m)$ где H_{out}, H_{in}, m — блоки длины 256 бит.

Входное сообщение M разделяется на блоки $m_n, m_{n-1}, m_{n-2,} \dots, m_1$ по 256 бит. В случае если размер последнего блока меньше 256 бит, то к нему приписываются слева нули для достижения заданной длины блока.

Каждый блок сообщения, начиная с первого, подаётся на шаговую функцию для вычисления промежуточного значения хеш-функции:

$$H_{i+1} = f(H_i, m_i)$$

Значение H_1 можно выбрать произвольным.

После вычисления H_{n+1} конечное значение хеш-функции получают следующим образом:

$H_{n+1} = f(H_{n+1}, L)$, где $L -$ длина сообщения M в битах по модулю 2^{256}

$h = f(H_{n+2}, K)$, где $K -$ контрольная сумма сообщения M: $m_1 + m_2 + m_3 + \cdots + m_n$

$h -$ значение хеш $-$ функции сообщения M

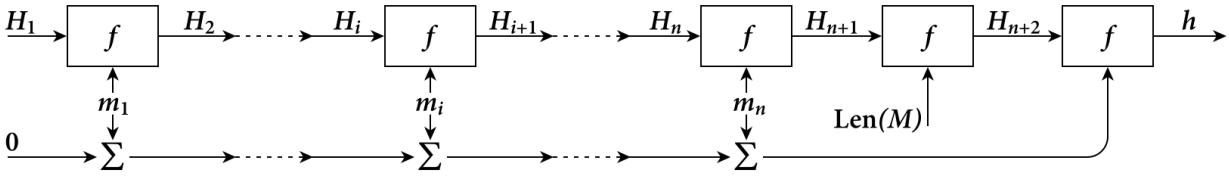

Рисунок 1 - Алгоритм хеш-функции ГОСТ 34.11-94

2. Примеры работы программы

Пример 1.

Исходное сообщение: «»

Хеш:«CE85B99CC46752FFFEE35CAB9A7B0278ABB4C2D2055CFF685AF4912C49490F8D»

Пример 2.

Исходное сообщение: «abc»

Хеш:«F3134348C44FB1B2A277729E2285EBB5CB5E0F29C975BC753B70497C06A4D51D»

Пример 3.

Исходное сообщение: «abc.»

Хеш:«50A3EB3B73229D7F50A25AED3DA5EE7C2E1520888FEB5FB5B21C71A490D79A29»

3. Результаты эксперимента

Для проведения эксперимента были придуманы следующие 3 слова-пароля: «abc», «my name is Sofi!», «000000000».

Таблица 1 – Результаты эксперимента

	abc	my name is Sofi!	000000000
2-й прообраз 2 бит	3.739	4.320	3.698
2-й прообраз 4 бит	15.932	15.968	15.887
2-й прообраз 6 бит	65.855	63.789	69.462
2-й прообраз 8 бит	261.701	271.128	256.675
Коллизия 2 бит	1.596	1.954	1.546
Коллизия 4 бит	11.183	11.412	10.909
Коллизия 6 бит	54.274	54.834	56.622
Коллизия 8 бит	245.220	236.815	231.731

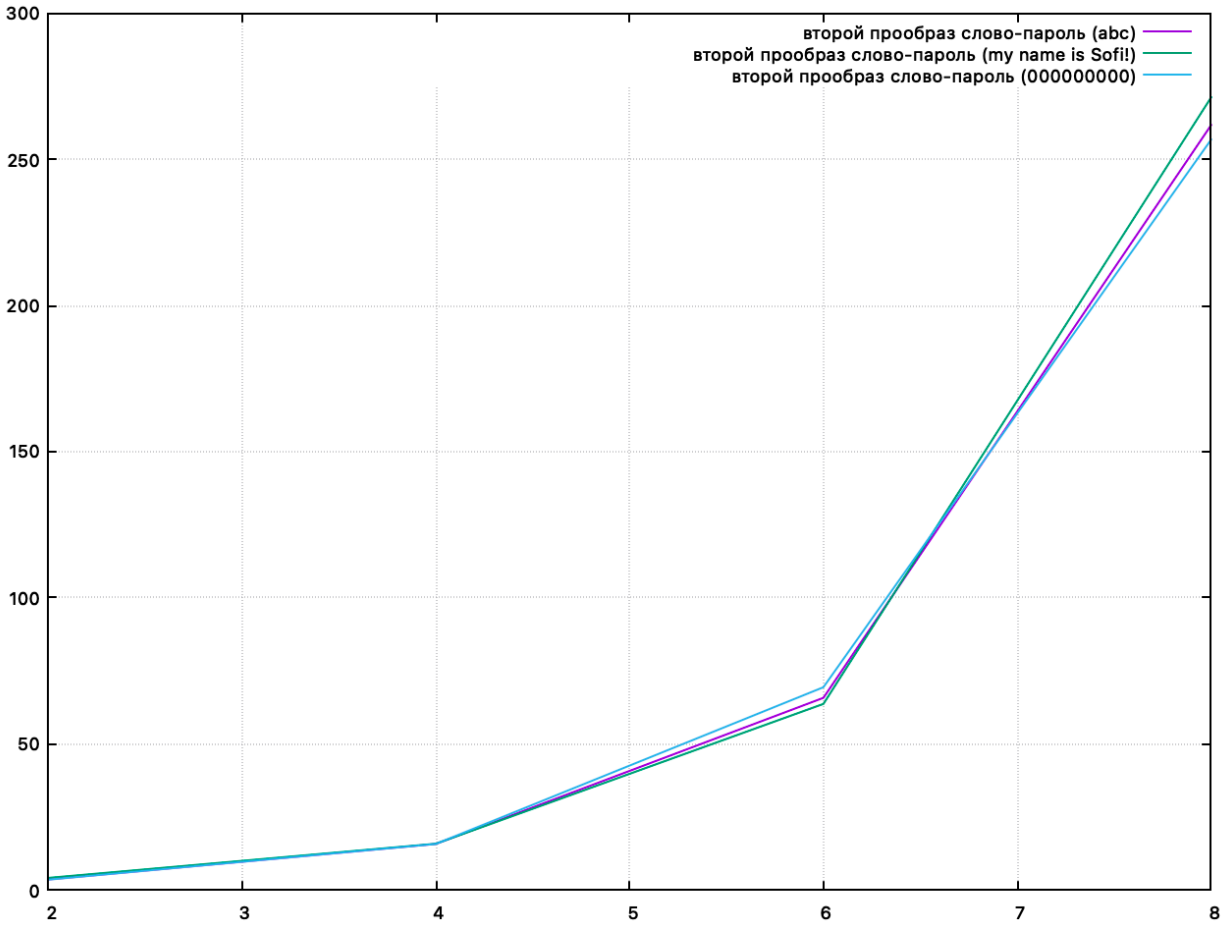

График 1 - График зависимости второго прообраза от количества взятых бит

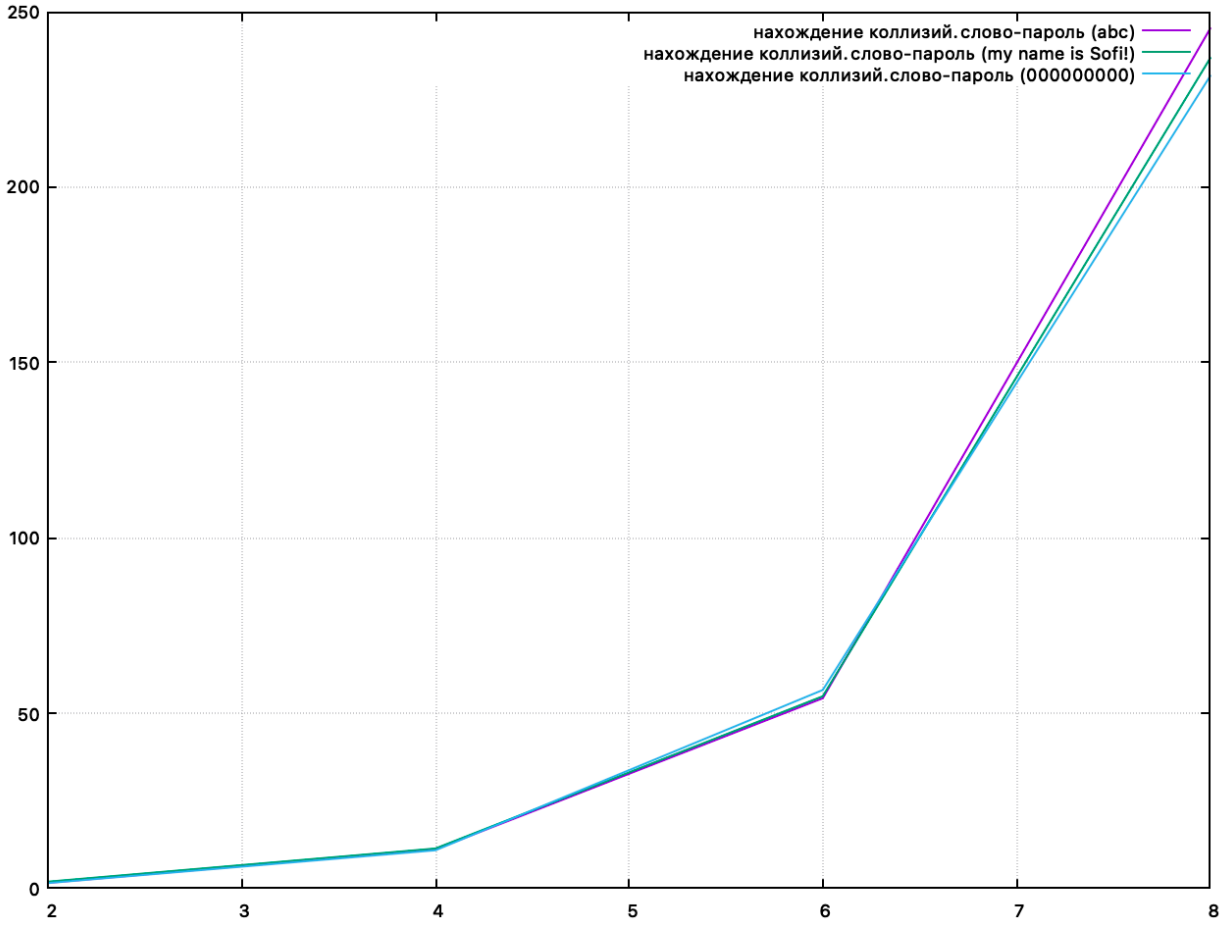

График 2 - График зависимости среднего значения сложности коллизии от количества взятых бит

Вывод

В ходе выполнения данной лабораторной работы был реализован алгоритм хеширования ГОСТ 34.11-94, а также проведен эксперимент.

Функция используется при реализации систем цифровой подписи, в сертификатах открытых ключей, для защиты сообщений в S/MIME и целостности Интернет адресов и имен.

В 2008 году командой экспертов из Австрии и Польши была обнаружена техническая уязвимость, сокращающая поиск коллизий в 2^{23} раз. Количество операций, необходимое для нахождения коллизии, таким образом, составляет 2^{105}, что, однако, на данный момент практически не реализуемо. Проведение коллизионной атаки на практике имеет смысл только в случае цифровой подписи документов, причём, если взломщик может изменять неподписанный оригинал.