Министерство образования Республики Беларусь

Учреждение образования «Белорусский государственный технологический университет»

Факультет информационных технологий

Кафедра информационных систем и технологий

**Отчет к лабораторной работе**:

Исследование асимметричных шифров RSA и Эль-Гамаля

Выполнил:

студент 3 курса 4 группы

специальности ПОИТ

Борисов А.А.

Минск 2021

1. **Теоретические сведения**

Определение 1. Хеш-функция – математическая или иная функция, h = H(М), которая принимает на входе строку символов М, называемую также прообразом, переменной длины n и преобразует ее в выходную строку фиксированной (обычно – меньшей) длины, l.

Определение 2. Хеширование (или хэширование, англ. hashing ) – это преобразование входного массива данных определенного типа и произвольной длины (практически) в выходную битовую строку фиксированной длины.

Преобразования называются хеш-функциями или функциями свертки, а их результаты называют хешем, хеш-кодом, хеш-таблицей или дайджестом сообщения (анг. message digest).

Теорема 1. Основная теорема арифметики. Всякое натуральное число N, кроме 1, можно представить как произведение простых множителей:

Определение 3. Криптографическая хеш-функция – это специальный класс хеш-функций, который имеет различные свойства, необходимые для решения задач в области криптографии. Основные задачи, решаемые с помощью хеш-функций:

• аутентификация (хранение паролей),

• проверка целостности данных,

• защита файлов,

• обнаружение зловредного ПО,

• криптовалютные технологии.

К основным свойствам хеш-функций можно отнести следющие.

Свойство 1. Детерминированность: независимо от того, сколько раз вычисляется H(M), M – const , при использовании одинакового алгоритма код хеш-преобразования h всегда должен быть одинаковым.

Свойство 2. Скорость вычисления хеша h: если процесс вычисления h не достаточно быстрый, система просто не будет эффективной.

Свойство 3: Сложность обратного вычисления: для известного H (М) невозможно (практически) определить М. Это важнейшее свойство хеш-функции для криптографических применений – односторонности преобразования.

Определение 5. Хеш-функция – это функция, выполняющая отображение из множества М в число, находящееся в интервале

[0, m–1]: h: M → [0, m–1]. (x mod pi) = ai ,

Алгоритмы семейства MD-x (2/4/5/6) являются творениями Р. Ривеста; MD – Message Digest. Алгоритм MD6, в отличие от предыдущих версий алгоритма этого семейства, не стандартизован.

Алгоритмы семейства SHA (SHA – Secure Hash Algorithm) являются в настоящее время широко распространенными. По существу во многих случаях завершился переход от SHA-1 к стандартам версии SHA-2. SHA-2 – собирательное название алгоритмов SHA-224, SHA256, SHA-384 и SHA-512. SHA-224 и SHA-384 являются, по сути, аналогами SHA-256 и SHA-512 соответственно.

Базовые алгоритмы обоих рассматриваемых семейств (MD и SHA) условно можно разделить на 5 стадий:

* расширение входного сообщения;
* разбивка расширенного сообщения на блоки;
* инициализация начальных констант;
* обработка сообщения поблочно (основная процедура алгоритма хеширования);
* вывод результата.

1. **Практическая часть**

В данной лабораторной работе необходимо разработать оконное приложение, реализующее один из алгоритмов хеширования из указанного преподавателем семейства (MD или SHA; или иного).

В связи с поставленными требованиями было разработано приложение реализующее алгоритм

Пример первого раунда хеш-функции:

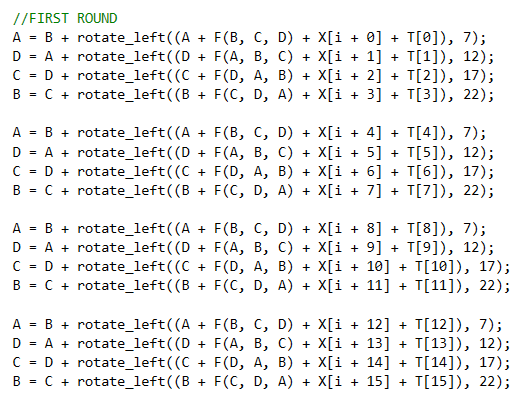


Рисунок 2.1 – Листинг раунда MD5

**Вывод**

В данной лабораторной работе я закрепил теоретические знания по хеш-функциям. А так же, разработал приложения по алгоритму MD5.