МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образование «Белорусский государственный технологический университет»

**«**Исследование криптографических хеш-функций**»**

Студент: Бутурля Р.А.

ФИТ 3 курс 5 группа

Вариант 3

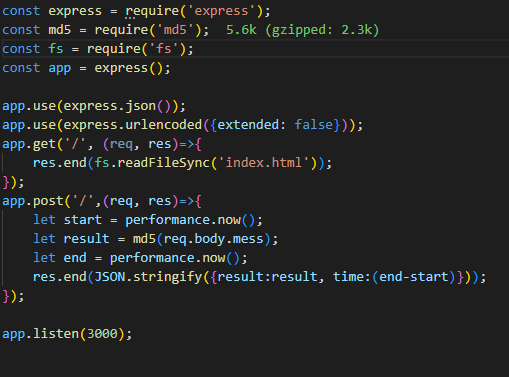
Преподаватель: Савельева М. Г.

Минск 2023

1. Разработать оконное приложение, реализующее один из алгоритмов хеширования из указанного преподавателем семейства (MD или SHA; или иного). При этом можно воспользоваться доступными готовыми библиотеками. Язык программирования – на свой выбор. Приложение должно обрабатывать входные сообщения, длина которых определяется спецификацией на реализуемый алгоритм.

Алгоритм хеширования – MD-5. Выбран он был по следующей причине: MD-5 – это MD-4 с улучшенным битовым хешированием, дополнительным этапом и улучшенным лавинным эффектом.

Для реализации приложения воспользуемся готовым пакетом решений – «md5» для Node.js. Код приложения представлен на листинге 1.



Листинг 1 – Код приложения

1. Оценить быстродействие выбранного алгоритма хеширования

Для определения быстродействия построим таблицу зависимости времени от длинны сообщения.

Таблица 1 – Зависимость времени выполнения операции от длинны сообщения

|  |  |  |  |
| --- | --- | --- | --- |
| Операция\длина сообщения | 32 | 64 | 128 |
| Хеширование | 0.827 | 0.23 | 0.12 |

По результатам таблицы построим гистограмму – рисунок 1.

Рисунок 1 –Зависимость времени он длинны сообщения

**Вывод**

Изучил алгоритмы хеширования и приобрел практические навыки их реализации и использования в криптографии.