УДК 004

Калашников Р.П.
магистр 2 курса, ЮРГПУ(НПИ) им. М.И Платова, г. Новочеркасск,
Комарова А.О.
магистр 2 курса, ЮРГПУ(НПИ) им. М.И Платова, г. Новочеркасск,
Воробьев С.П.
к.т.н., доцент каф. ИИСТ, ЮРГПУ(НПИ) им. М.И Платова,
г. Новочеркасск, РФ

ЭКСПЕРИМЕНТАЛЬНОЕ ИССЛЕДОВАНИЕ БЫСТРОДЕЙСТВИЯ АЛГОРИТМОВ ШИФРОВАНИЯ ДАННЫХ

Аннотация: *В статье рассматриваются ГОСТ Р 34.11-2012 и SHA-256, так как они имеют одинаковую по длине выходной результат. Данные алгоритмы выбраны в связи с политикой импортозамещения. Выполняется построение графиков на основании результатов.*

Ключевые слова: *шифрование данных, шифрование, быстрый алгоритм хеширования, хеширование, алгоритм хеширования.*

Annotation: *In the article GOST R 34.11-2012 and SHA-256 are considered, since they have the same output in length. These algorithms have been chosen in connection with the policy of import substitution. The construction of graphs based on the results.*

Key words: *encryption, encryption, fast hashing algorithm, hashing, hash algorithm.*

В высокотехнологичном информационном обществе использование средств защиты информации является жизненно необходимым, поскольку это позволяет реализовать такие свойства защищаемых данных, как конфиденциальность, целостность, аутентичность, которые обеспечиваются с помощью методов криптографии.

SHA-256 реализует хеш-функцию, построенную на идее функции сжатия. Входами функции сжатия являются блок сообщения длиной 265 бит и выход предыдущего блока сообщения. Выход представляет собой значение всех хеш-блоков до этого момента. Иными словами хеш блока M{i} равен h{i}=f(M{i},h{i-1}). Хеш-значением всего сообщения является выход последнего блока.[1]

ГОСТ Р 34.11-2012 «Стрибог» — Информационная технология криптографической защиты информации, функция хэширования, действующий российский криптографический стандарт, определяющий алгоритм и процедуру вычисления хеш-функции. Разработан Центром защиты информации и специальной связи ФСБ России с участием ОАО «ИнфоТеКС» и введенный в действие 1 января 2013 года.

В основу хеш-функции положена итерационная конструкция Меркла-Дамгарда с использованием MD-усиления. Под MD-усилением понимается дополнение неполного блока при вычислении хеш-функции до полного путём добавления вектора (0 … 01) такой длины, чтобы получился полный блок.

Стандарт определяет алгоритм и процедуру вычисления хеш-функции для последовательности символов. Этот стандарт разработан и введён в качестве замены устаревшему стандарту ГОСТ Р 34.11-94. Как было заявлено в ФСБ России:

«Необходимость разработки вызвана потребностью в создании хеш-функции, соответствующей современным требованиям к криптографической стойкости и требованиям стандарта ГОСТ Р 34.10-2012». [2]

Начальный экран программы представлен на рисунке 1.

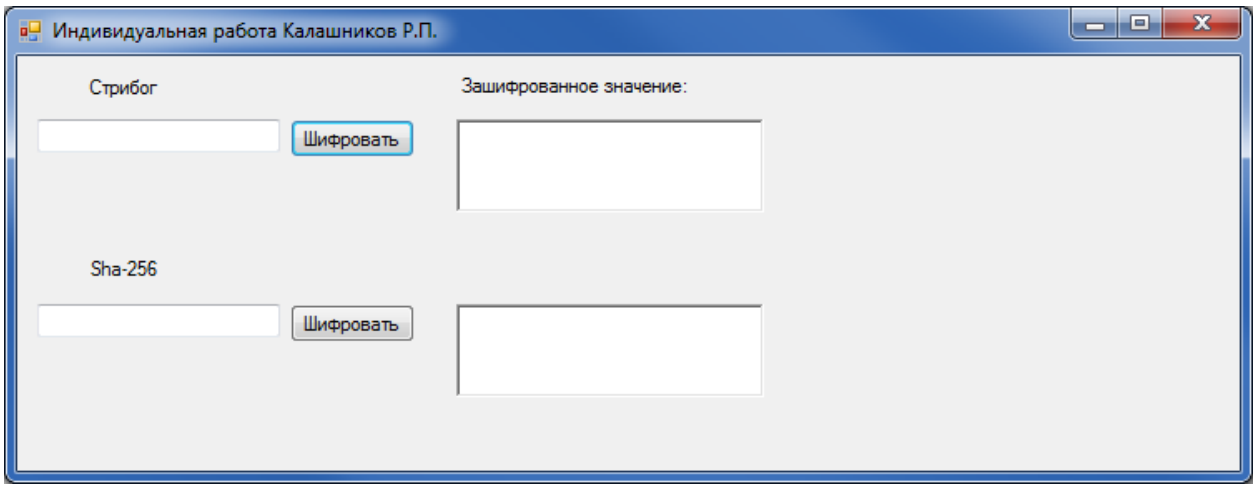

Рисунок 1 – Начальный экран программы

Далее вводим одинаковые слова для шифрования, чтобы узнать скорость формирования хэша и эксперимент был более корректным, проведем 5 опытов, представлены на рисунках 2-6.

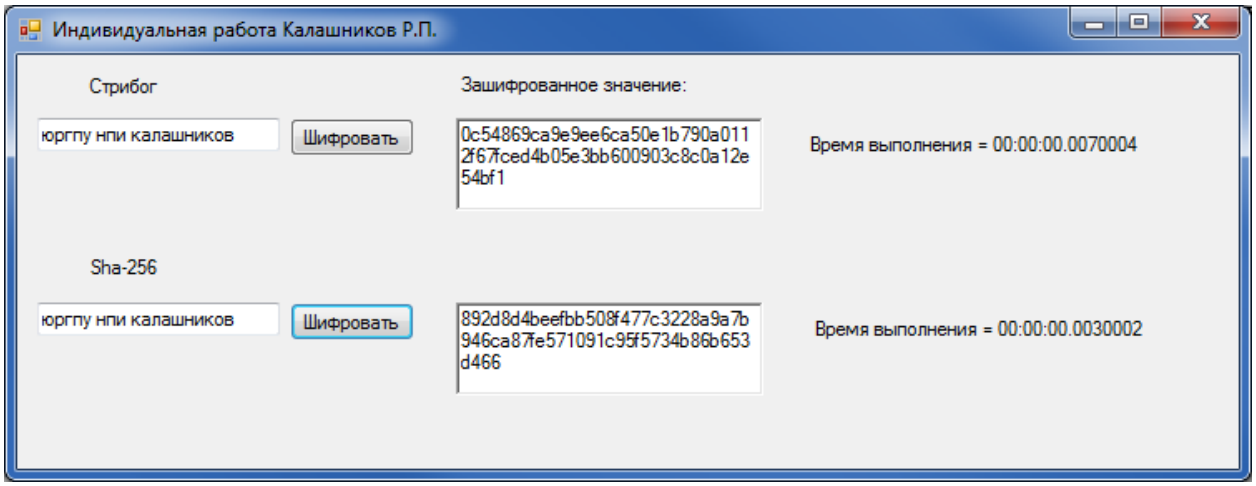

Рисунок 2 – Опыт 1

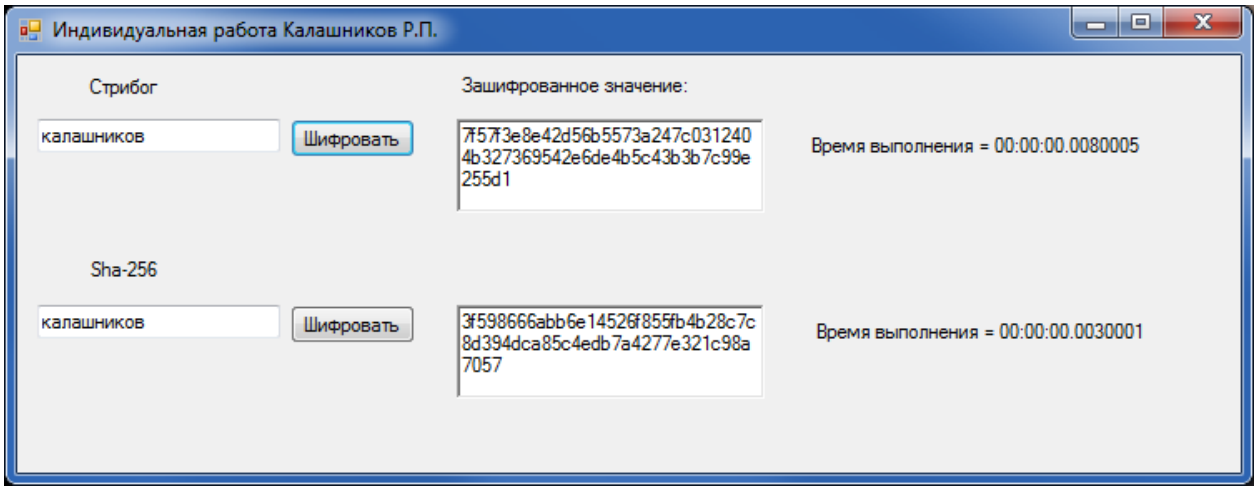

Рисунок 3 – Опыт 2

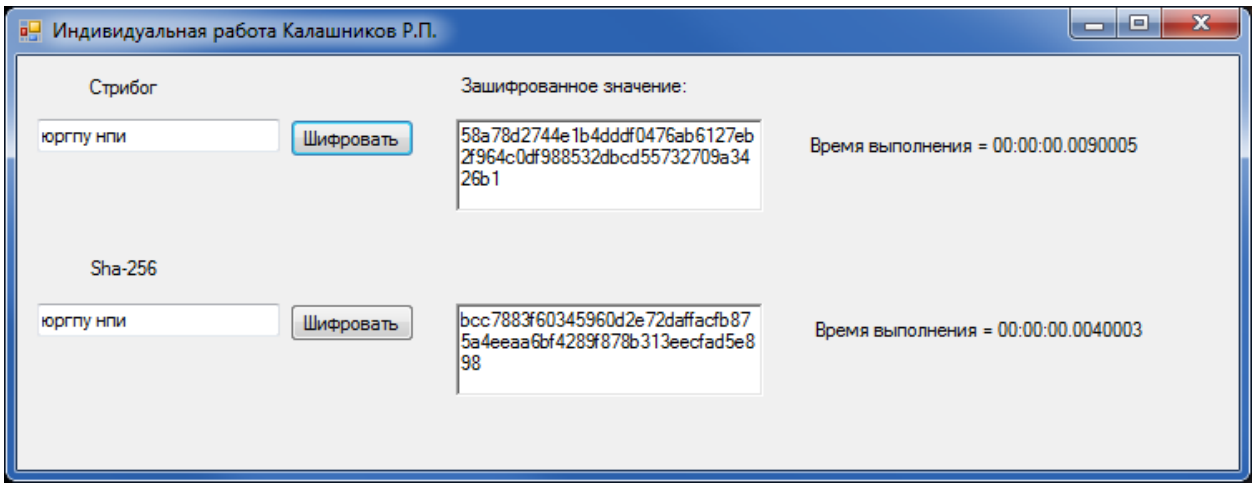

Рисунок 4 – Опыт 3

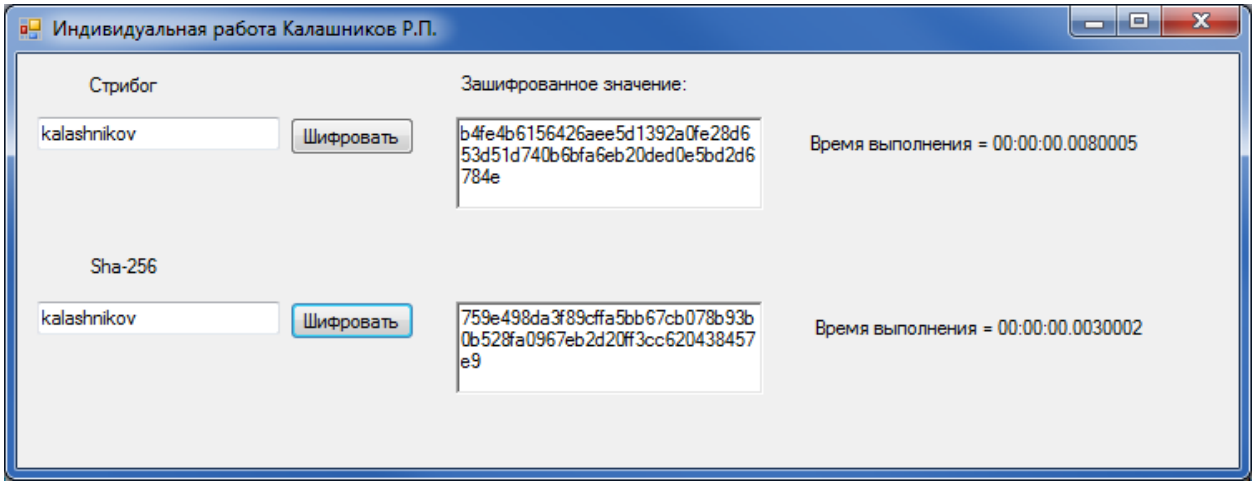

Рисунок 5 – Опыт 4

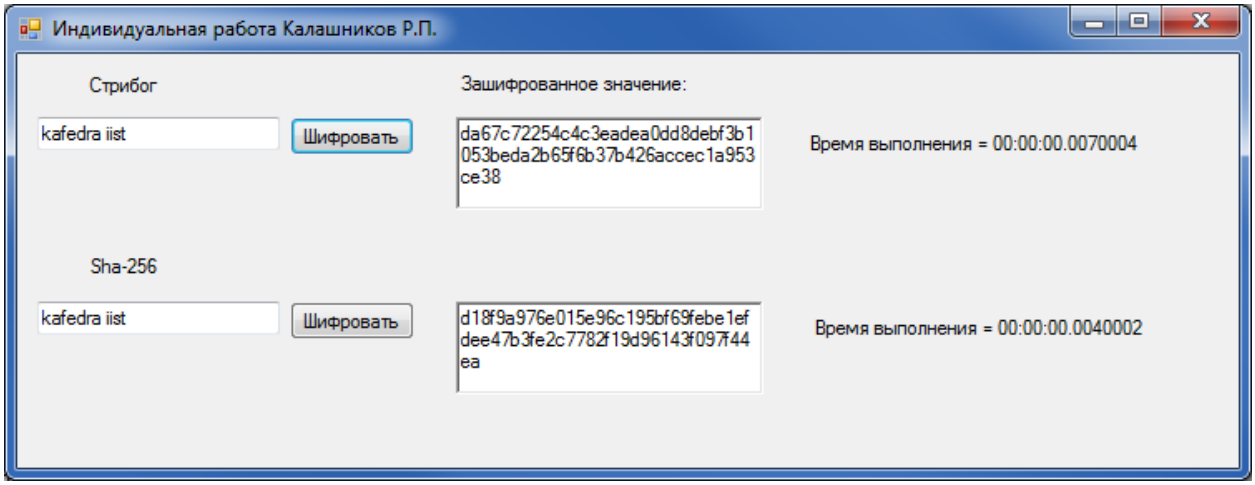

Рисунок 6 – Опыт 5

Листинг программы представлен в приложении Б.

В таблице 1 представлены данные, полученные в результате выполнения программы, с использованием эвристического метода, при различных запросах в строке для ввода слов.

Таблица 1 – Результат эксперимента при различных запросах в строке для ввода слов.

Опыт №	Запрос	Стрибог, (сек)	SHA-256, (сек)
1	юргпу нпи калашников	0,00700004	0,00300002
2	калашников	0,00800005	0,00300001
3	юргпу нпи	0,00900005	0,00400003
4	kalashnikov	0,00800005	0,00300002
5	kafedra iist	0,00700004	0,00400002

На основании данных, приведенных в таблице 1 построен график зависимости времени затраченного на построения хеша от введенного запроса, представленный на рисунке 7.

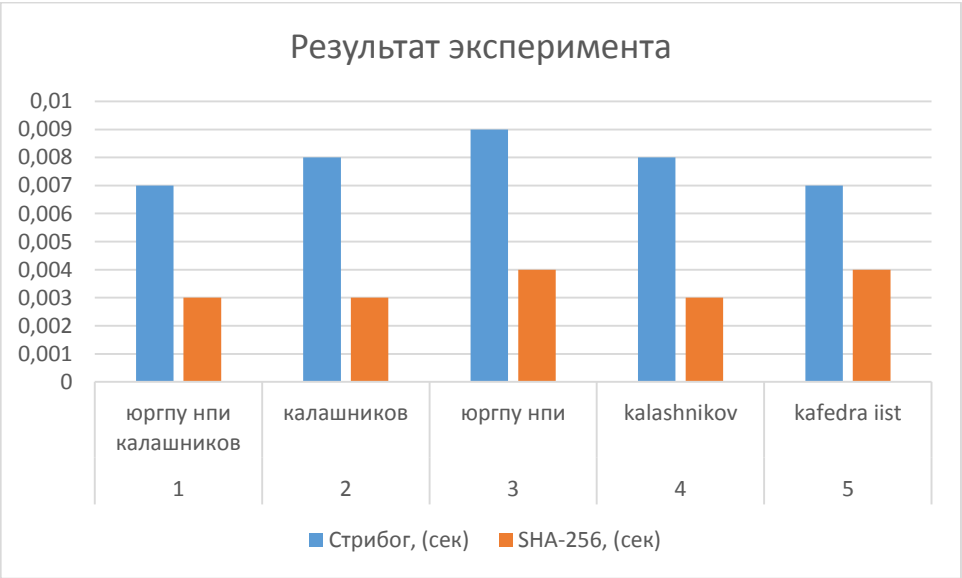

Рисунок 7 – Результаты эксперимента зависимости скорости формирования хеша от введенного запроса

С помощью данной программы было проведено 5 опытов в ходе которых на вход функций были введены слова и замерялось время выполнения для каждой из функций хеширования.

По данным опытов были построены гистограмма и таблица, по данным которых можно сделать вывод, что SHA-256 работает быстрее, чем Стрибог.

Использованные источники:

1. ГОСТ Р 34.11-2012 — Википедия [Электронный ресурс] – https://ru.wikipedia.org/wiki/ГОСТ_Р_34.11-2012 (дата обращения 10.03.2018);
2. SHA-256 — Википедия [Электронный ресурс] – https://ru.wikipedia.org/ ru.wikipedia.org/wiki/SHA-256 (дата обращения 11.03.2018).