Учреждение образования

«Белорусский государственный технологический университет»

**Кафедра информационных систем и технологий**

**«Отчёт по лабораторной работе 11»**

“ Исследование криптографических хеш-функций”

**Выполнила:** студентка 3 курса

4 группы специальности ПОИТ

Сапегина Екатерина Игоревна,

Вариант 11 (1)

Минск 2023

***Цель:*** изучение алгоритмов хеширования и приобретение практических навыков их реализации и использования в криптографии.

***Задачи:***

1. Закрепить теоретические знания по алгебраическому описанию и алгоритмам реализации операций вычисления однонаправленных хеш-функций.

2. Освоить методику оценки криптостойкости хеш-преобразований на основе «парадокса дня рождения».

3. Разработать приложение для реализации заданного алгоритма хеширования (из семейств MD и SHA).

4. Оценить скорость вычисления кодов хеш-функций.

5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

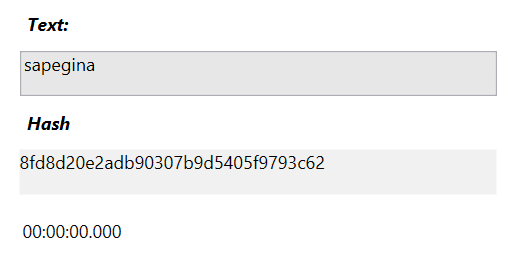
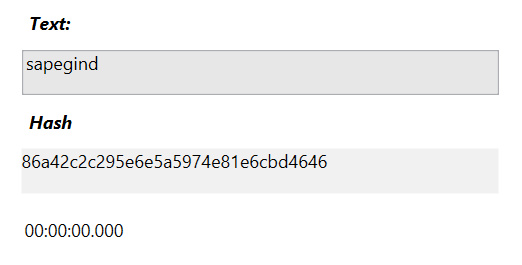
***Практическая часть:***

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.

***Реализация MD5:***

|  |
| --- |
| output.Text = "";  byte[] hash = Encoding.ASCII.GetBytes(input.Text);  MD5 md5 = new MD5CryptoServiceProvider();  var startTime = System.Diagnostics.Stopwatch.StartNew();  byte[] hashenc = md5.ComputeHash(hash);  startTime.Stop();  var resultTime = startTime.Elapsed;  string elapsedTime = String.Format("{0:00}:{1:00}:{2:00}.{3:000}",  resultTime.Hours,  resultTime.Minutes,  resultTime.Seconds,  resultTime.Milliseconds);  foreach (var b in hashenc)  {  output.Text += b.ToString("x2");  }  time.Text = elapsedTime; |

***Результат:***

****** ******