**Лабораторная работа № 8**

**Исследование потоковых шифров**

**Цель:** изучение и приобретение практических навыков разработки и использования приложений для реализации потоковых шифров.

**Задачи**:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости потоковых шифров.

2. Разработать приложение для реализации указанных преподавателем методов генерации ключевой информации и ее использования для потокового зашифрования/расшифрования.

3. Выполнить анализ криптостойкости потоковых шифров.

4. Оценить скорость зашифрования/расшифрования реализованных шифров.

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

**Вариант 15 (5)**.

**Основное** **задание**.

1. Разработать авторские многооконные приложения в соответствии с целью лабораторной работы. При этом можно воспользоваться готовыми библиотеками либо программными кодами, реализующими заданные алгоритмы.

*Приложение 1* должно реализовывать генерацию ПСП в соответствии с вариантом из табл.

|  |  |  |
| --- | --- | --- |
| 5 | Линейный конгруэнтный генератор | а = 421, с = 1663, n = 7875 |

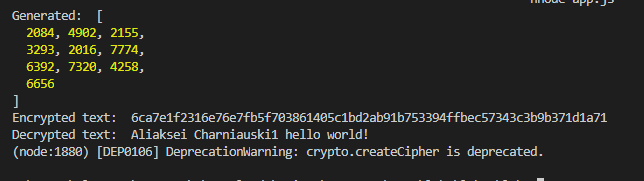
*Приложение 2* должно реализовывать алгоритм RC4 в соответствии с вариантом из табл.

|  |  |  |
| --- | --- | --- |
| 15 | 8 | 1, 11, 21, 31, 41, 51 |

В качестве шифруемого сообщения может быть выбран произвольный текст

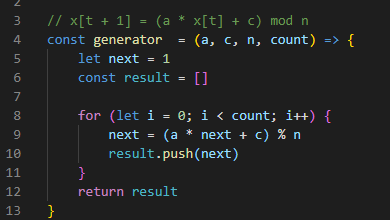
2. Результаты оформить в виде отчета по установленным правилам.

**Результат работы:**



**Листинги:**

Функция генерации псевдослучайных чисел:



Функция RC4:

