**Лабораторная работа №2. Криптографические алгоритмы.**

1. Реализуйте поточный шифр для шифрования/расшифрования строки, введённой с клавиатуры (выбрать вариант из таблицы 1).
2. Реализуйте блочный шифр для шифрования/расшифрования файлов (выбрать вариант из таблицы 2).
3. Реализуйте один из алгоритмов построения хеш-функции на основе разработанного блочного шифра.

Таблица 1 - алгоритмы к заданию 1

|  |  |
| --- | --- |
| **№** | **Алгоритм** |
| 1 | RC4 |
| 2 | Salsa20 |
| 3 | Vernam cipher |
| 4 | Caesar Cipher |
| 5 | Поточный шифр на основе ЛКГ |

Таблица 2 - алгоритмы к заданию 2

|  |  |
| --- | --- |
| № | **Алгоритм** |
| 1 | AES |
| 2 | Кузнечик |
| 3 | ГОСТ 28147-89 |
| 4 | CLEFIA |
| 5 | IDEA |
| 6 | RC5 |
| 7 | Simon |
| 8 | Skipjack |
| 9 | Speck |
| 10 | Present |

**Выбор варианта: порядковый номер в группе % (количество вариантов + 1)**