# Лабораторная работа № 3
# Статистическое тестирование псевдослучайных последовательностей

**Базовое задание** (4 *балла, дата сдачи* ≤ *01.06.2020*).

Осуществить моделирование псевдослучайной бинарной последовательности, используя линейный конгруэнтный генератор. Для оценки качества выходной последовательности реализовать один из трех тестов, описанных в [1] (вариант см. в таблице). Реализовать тестирование последовательности из текстового файла (пример файла прилагается – e.txt).

**Дополнительные задания** (принимаются при условии, что сдано основное задание, *i*-ое дополнительное задание принимается при условии, что сданы дополнительные задания 1,..., *i*–1, *i* = 2, 3,...).

**1.** (2 *балла, дата сдачи* ≤ *20.04.2020*). Выполнить базовое задание для генератора Макларена-Марсальи.

**2.** (2 *балла, дата сдачи* ≤ *20.04.2020*). Выполнить базовое задание для регистра сдвига и самосжимающего генератора, реализовать два теста.

**3.** (1 *балл, дата сдачи* ≤ *13.04.2020*). Реализовать все три теста.

**4.** (1+4 *балла, дата сдачи* ≤ *06.04.2020*) Дешифровать файл с текстом (формат fb2), зашифрованный с помощью регистра сдвига с линейной обратной связью (файл прилагается). Характеристический многочлен регистра сдвига

$$f(x) = x^{16} + x^{15} + x^{12} + x^{10} + 1.$$

Пример шифрования:

начальное состояние регистра (в двоичном представлении): 1000000000000001

байты открытого текста: 33 2E 2C 64 32 67 34 76

байты шифрующей гаммы: 80 01 19 5E F6 B5 AC 8A

байты шифртекста: B3 2F 35 3A C4 D2 98 FC

## Литература

1. A statistical test suite for random and pseudorandom number generators for cryptographic applications: NIST Special Publication 800-22 Rev. 1a. – National Institute of Standards and Technology, 2010. – 131 p.

| Фамилия, Имя | Тесты |
|---|---|
| Гуляев Владислав | 5, 10, 11 |
| Дрепакова Ангелина | 2, 3, 14 |
| Ермолаева Екатерина | 1, 10, 14 |
| Калинчук Иван | 4, 5, 7 |
| Клещёв Максим | 7, 9, 11 |

| | |
|---|---|
| Коновалова Валерия | 3, 4, 5 |
| Лиховец Максим | 10, 11, 12 |
| Матвеёнок Алексей | 7, 13, 14 |
| Махницкий Никита | 1, 5, 15 |
| Федченко Юрий | 2, 8, 10 |
| Шаршнёв Максим | 9, 13, 15 |
| Шишлянников Иван | 4, 8, 9 |