Лабораторная работа 5: «Изучение свойств мультипликативной группы расширенного поля Галуа» [до 19 мая]

1. О деталях реализации и средствах разработки

- Основной прием шифрования и дешифрования в поточных шифрах (Java):

```
int x = 123;
System.out.println(Integer.toBinaryString(x));

//Исключающее ИЛИ (побитовое сложение по модулю два)
System.out.println(Integer.toBinaryString(x^28^28));
```

2. Постановка задачи

Реализуйте генератор псевдослучайной последовательности битов на основе регистра сдвига с линейной обратной связью (РСЛОС) в конфигурации Галуа. Начальное значение сдвигового регистра и его образующий многочлен должны задаваться пользователем. Результат представьте в виде точечной диаграммы, где по горизонтали отложены порядковые номера генерируемых битов, а по вертикали – их значения. С помощью критерия χ^2 оцените качество любой генерируемой последовательности, длина которой кратна максимальной. Путем однократного гаммирования, не затрагивая заголовочную часть, зашифруйте изображение `tux.png` (формат не принципиален), порциями по 8 бит. Объясните результат.

3. Задания для подготовки к экзамену

1. Напишите программу, реализующую процедуру MixColumns шифра AES (длина блока равна 128 битов). Входные и выходные данные должны быть представлены в виде квадрата (в учебных целях).

2. Напишите программу, реализующую процедуры для контроля целостности произвольного сообщения на основе CRC (циклического избыточного кода) по произвольному порождающему полиному. С помощью программы должно быть возможно как добавить кон-

трольную сумму к сообщению, так и проверить по сумме целостность сообщения[1].

[1]Алгоритм контрольного суммирования CRC широко используется в устройствах хранения данных и в проводных и беспроводных сетях для проверки информации на подлинность и ее защиты от несанкционированного изменения. Эффективен для обнаружения ошибок в данных при случайных изменениях (в результате сбоев или помех), но не в случаях преднамеренных вмешательств.