Задания к работе №3 по основам криптографии.

Все задания выполняются на объектно-ориентированном языке программирования.
Применение готовых реализаций алгоритмов защиты информации и библиотек, содержащих такие реализации, не допускается.

1. Реализуйте stateless-сервис, предоставляющий объектный функционал для:
   - сложения двоичных полиномов (далее - элементов) из $GF(2^8)$;
   - умножения элементов из $GF(2^8)$ по заданному модулю;
   - взятия обратного элемента для элемента из $GF(2^8)$ по заданному модулю;
   - проверки двоичного полинома степени 8 на неприводимость над $GF(2^8)$;
   - построения коллекции всех неприводимых над $GF(2^8)$ двоичных полиномов степени 8 (спойлер: их должно получиться 30);
   - построения разложения двоичного полинома произвольной степени на неприводимые множители из $GF(2^n)$, $n \in N$.

   При попытке выполнения операции умножения/взятия обратного элемента по приводимому над $GF(2^8)$ модулю, генерируйте (и перехватывайте в вызывающем коде) исключительную ситуацию. Значения элементов из $GF(2^8)$ и модулей над $GF(2^8)$ передавайте и возвращайте в виде однобайтовых значений (byte, char, … (в зависимости от используемого языка программирования)). При вычислениях максимизируйте использование битовых операций.

2. На базе интерфейсов 2.1, 2.2, 2.3 (см. Задания к работе №1 по защите информации, задание 2) реализуйте класс, функционал которого позволяет выполнять [де]шифрование блока данных алгоритмом Rijndael. Обеспечьте возможность переиспользования для [де]шифрования различных блоков данных ключей раунда, полученных в результате выполнения процедуры расширения ключа. Реализация алгоритма должна поддерживать работу с блоками длиной 128/192/256 бит и ключами длиной 128/192/256 бит, а также предоставлять возможность настройки модуля над $GF(2^8)$ на этапе конструктора (используйте функционал, реализованный в задании 1). S-матрицы, необходимые для выполнения работы алгоритма, необходимо отложенно инициализировать для настроенного модуля над $GF(2^8)$. Вычисление прямой S-матрицы через обратную и

наоборот не допускается. При работе с элементами из $GF(2^8)$ используйте функционал, реализованный в задании 1.

3. Продемонстрируйте выполнение шифрования и дешифрования псевдослучайных последовательностей байтов и файлов (текстовых, музыкальных, изображений, видео и т. д.) реализованным в задании 2 функционалом с использованием различных режимов шифрования и различных режимов набивки (см. Задания к работе №1 по защите информации, задание 4), различных длины блока и длины ключа, а также с использованием различных неприводимых над $GF(2^8)$ двоичных полиномов степени 8.