Лабораторная работа №3

**Изучение криптографических алгоритмов.**

**Алгоритмы шифрования.**

Задание

1. Реализовать указанный преподавателем криптографический алгоритм.
2. Программа должна иметь интерфейс, в котором содержатся данные студента, вариант, справочная информация – алгоритм и его описание, возможности для сохранения и выбора обрабатываемого файла.
3. В случае шифрования пароль должен вводиться как с клавиатуры, так и из файла по выбору.
4. Отчет должен содержать вариант задания, блок-схему алгоритма, реализованного в программе, листинг программы с комментариями, расчет данных по одному циклу алгоритма.
5. Отчет и код программы с исполняемым кодом дополнительно представляются в электронном виде.
6. Обрабатываться должен файл любого формата(word,excel, графические форматы и т.д.), длиной не менее 1 кБ.
7. В программе должна быть возможность выбора исходного файла и файла назначения как для шифрования, так и для расшифрования.
8. Ответить на вопросы преподавателя.

**Вопросы:**

1. Симметричные алгоритмы шифрования и их характеристики.
2. Асиметричные алгоритмы шифрования и их характеристики.
3. Реализация хэш-функций.
4. Реализация MAC.
5. Реализация ЭЦП.
6. Понятие слоя, раунда, S-box.
7. Как в ГОСТ Р 34.12-2018Магма (ГОСТ 28147) осуществляется преобразование с помощью S-boxes. Что подается на вход и получается на выходе.

**Варианты:**

1. Алгоритм DES в режиме ECB (Electronic Codebook) - электронный шифроблокнот.
2. Алгоритм DES в режиме CBC (Cipher Block Chaining) - цепочка блоков.
3. Алгоритм DES в режиме CFB (Cipher Feedback) - обратная связь по шифртексту.
4. Алгоритм DES в режиме OFB (Output Feedback) - обратная связь по выходу.
5. Алгоритм ГОСТ Р 34.12-2018 Магма (ГОСТ 28147). Режим гаммирования.
6. Алгоритм ГОСТ Р 34.12-2018 Магма (ГОСТ 28147). Режим гаммирования с ОС.
7. Алгоритм ГОСТ Р 34.12-2018 Магма (ГОСТ 28147). Режим простой замены.