Лабораторная работа 1 по основам криптографии.

1. Реализуйте функцию для выполнения перестановки битов в рамках переданного значения (тип - массив байтов). Параметры функции: значение для перестановки, правило перестановки (P-блок).

2. Реализуйте функцию для выполнения замены группы битов размера *k* на другую группу битов размером *k* в рамках переданного значения (тип - массив байтов). Параметры функции: значение для перестановки, правило перестановки (S-блок), размер входной группы *k* (в битах).

3. Спроектируйте следующие сущности:

   1. интерфейс, предоставляющий описание функционала для процедуры расширения ключа (генерации раундовых ключей) (параметр метода: входной ключ - массив байтов, результат - массив раундовых ключей (каждый раундовый ключ - массив байтов));

   2. интерфейс, предоставляющий описание функционала по выполнению шифрующего преобразования (параметры метода: входной блок - массив байтов, раундовый ключ - массив байтов, результат: выходной блок - массив байтов);

   3. интерфейс, предоставляющий описание функционала по выполнению шифрования и дешифрования симметричным алгоритмом (параметр методов: [де]шифруемый блок (массив байтов)) с преднастроенными отдельным методом раундовыми ключами (параметр метода: ключ [де]шифрования (массив байтов));

   4. класс-контекст, предоставляющий объектный функционал по выполнению шифрования и дешифрования симметричным

алгоритмом (реализацией интерфейса из п. 3) с поддержкой одного из режимов шифрования (задаётся перечислением): ECB, CBC, CFB, OFB, CTR, RD, RD+H. Параметры конструктора класса: ключ шифрования, режим шифрования (объект перечисления), вектор инициализации (опционально), дополнительные параметры для указанного режима (список аргументов переменной длины). Параметры методов шифрования/дешифрования: данные для шифрования (массив байтов произвольной длины и ссылка на результирующий массив байтов, либо путь к файлу со входными данными и путь к файлу с результатом [де]шифрования). Где возможно, реализуйте распараллеливание вычислений. Шифрование должно производиться асинхронно. При реализации используйте тип набивки (padding) PKCS7.

4. На базе интерфейса 3.3 спроектируйте класс, реализующий функционал сети Фейстеля. Конструктор класса должен принимать в качестве параметров реализации интерфейсов 3.1 и 3.2.

5. Реализуйте алгоритм шифрования DES на базе класса из задания 4, определив свои реализации интерфейсов 3.1 и 3.2. При реализации DES используйте функции, реализованные в заданиях 1 и 2.

6. Продемонстрируйте выполнение шифрования и дешифрования псевдослучайных последовательностей байтов и файлов (текстовых, музыкальных, изображений, видео) алгоритмом DES с использованием различных режимов шифрования.