Задания к работе №1 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 функцию для выполнения перестановки битов в рамках переданного значения (тип значения - массив байтов). Параметры функции: значение для перестановки, правило перестановки (P-блок), правила индексирования битов: биты индексируются от младшего к старшему или наоборот; номер начального бита == 0 или == 1.

2. 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, репрезентирующий контекст выполнения симметричного криптографического алгоритма, предоставляющий объектный функционал по выполнению операций шифрования и дешифрования заданным ключом симметричного алгоритма (реализацией интерфейса из п. 3) с поддержкой одного из режимов шифрования (задаётся перечислением): ECB, CBC, PCBC, CFB, OFB, CTR, Random Delta; а также с поддержкой одного из режимов набивки (задаётся перечислением): Zeros, ANSI X.923, PKCS7, ISO 10126. Параметры конструктора объекта класса: ключ шифрования, режим шифрования (объект перечисления), режим набивки (объект перечисления), вектор инициализации для заданного режима (опционально), дополнительные параметры для указанного режима (коллекция аргументов переменной длины). Параметры перегруженных методов шифрования/дешифрования: данные для [де]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. Выполнение операций шифрования/дешифрования должно производиться асинхронно.

3. На базе интерфейса 2 из задания спроектируйте и реализуйте класс, реализующий функционал сети Фейстеля. Конструктор класса должен принимать в качестве параметров реализации интерфейсов 2.1 и 2.2.

4. Реализуйте алгоритм шифрования DES на базе класса из задания 3, определив свои реализации интерфейсов 2.1 и 2.2. При реализации DES используйте функцию, реализованную в задании 1.

5. Продемонстрируйте выполнение шифрования и дешифрования псевдослучайных последовательностей байтов и файлов (текстовых, музыкальных, изображений, видео, файлов исходного кода тестов на аллокатор на базе красно-чёрного дерева и т. д.) алгоритмом DES с использованием различных режимов шифрования при помощи типов, реализованных в заданиях 2-4.

6. Реализуйте алгоритм шифрования DEAL на базе класса из задания 3, определив свои реализации интерфейсов 2.1 и 2.2. Для внедрения Вашей реализации алгоритма DES в алгоритм DEAL реализуйте адаптер, позволяющий использовать реализации алгоритма DES в качестве раундовой функции F.

7. Продемонстрируйте выполнение шифрования и дешифрования псевдослучайных последовательностей байтов и файлов (текстовых, музыкальных, изображений, видео, файлов исходного кода тестов на умножение Шёнхаге-Штрассена и т. д.) алгоритмом DEAL с использованием различных режимов шифрования при помощи типов, реализованных в заданиях 2-6.