Задания к работе №2 по кодированию и защите информации.

Все задания выполняются на языке программирования C++ (стандарт C++14 и выше).

Допускается использование библиотеки стандартных шаблонов (STL).

Применение готовых реализаций алгоритмов защиты информации и библиотек/фреймворков/прочих сторонних решений, содержащих такие реализации, не допускается.

Аварийное завершение работы реализованных компонентов и приложений не допускается.

Весь реализованный Public API компонентов должен быть покрыт модульными (unit-) тестами.

Реализация должна быть опубликована в репозиторий на GitHub.

Крайний срок публикации реализаций на GitHub: 26.02.2026 09:00 GMT+3.

1. Спроектируйте следующие интерфейсы:
    a. 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));
    b. интерфейс, предоставляющий описание функционала по выполнению шифрующего преобразования сети Фейстеля (параметры метода для выполнения шифрующего преобразования: входной блок - массив байтов, раундовый ключ - массив байтов, результат: выходной блок - массив байтов);
    c. 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));
    d. класс, реализующий функционал сети Фейстеля, с конфигурированием через конструктор реализаций интерфейсов из пунктов 1.a и 1.b, а также настройкой через конструктор количества раундов.
2. Реализуйте интерфейс-обёртку над классом 1.d, реализующий интерфейс 1.c и паттерн проектирования “Шаблонный метод”, функционал которого позволяет выполнить шифрование сетью Фейстеля, а также настроить дополнительные шаги до и после выполнения шифрования сетью Фейстеля.

3. Реализуйте интерфейс из задания 2 (реализация алгоритма DES), сконфигурировав функционал шаблонного метода для выполнения начальной и конечной перестановки уровня алгоритма DES. Реализации интерфейсов 1.a и 1.b для алгоритма DES должны являться вложенными (nested) по отношению к реализованному классу.
4. На основе реализованного в задании 3 класса реализуйте алгоритм 3DES с поддержкой интерфейса 1.c. Предусмотрите различные режимы выполнения алгоритма: DES-EEE3, DES-EDE3, DES-EEE2, DES-EDE2.
5. Реализуйте класс, объекту которого через конструктор передаётся реализация симметричного алгоритма шифрования. Функционал класса должен обеспечивать шифрование и дешифрование последовательностей байт уровня выполняющегося процесса, а также файлов, доступ к которым организуется по путям уровня файловой системы.
6. На основе реализованного в задании 5 класса продемонстрируйте выполнение шифрования и дешифрования псевдослучайных последовательностей байтов и файлов (текстовых, музыкальных, изображений, видео, исполняемых файлов, исходного кода задач по теории вероятностей и др.) алгоритмами DES и 3DES (с различными режимами выполнения 3DES).