Задание к курсовому проекту по основам криптографии.

1. Реализовать два симметричных алгоритма шифрования, реализующих интерфейс симметричного алгоритма шифрования (использование сторонних реализаций алгоритмов не допускается).

2. Реализовать протокол Диффи-Хеллмана (использование сторонних реализаций протокола не допускается).

3. Реализовать консольное серверное приложение, взаимодействие с которым возможно при помощи сетевого протокола и надстроек над ним (REST API, gRPC, WCF, etc.), API которого предусматривает возможность выполнения следующих протоколов (протокол может быть организован посредством выполнения нескольких связанных запросов):

- Создание “комнаты” для организации защищённого обмена сообщениями между двумя клиентами (секретный чат) с возможностью выбора используемого алгоритма шифрования из реализованных в п. 1;
- Закрытие ранее созданного секретного чата;
- Подключение и отключение клиентов от секретного чата;
- Организация распределения сеансового ключа симметричного алгоритма, сгенерированного посредством протокола Диффи-Хеллмана;
- Обработка пользовательских запросов на приём и передачу данных между клиентами, участвующими в защищённом обмене сообщениями.

Взаимодействие с сервером должно быть реализовано в асинхронном стиле с использованием брокера сообщений (Redpanda, Apache Kafka, Apache ActiveMQ Artemis, RabbitMQ, MSMQ и т. д.), предоставляющего очередь сообщений, producer и consumer которой находятся на стороне серверного приложения. Сообщениями, поступающими в брокер, должны являться фрагменты шифротекста. После передачи зашифрованного фрагмента сообщения клиенту-потребителю запрещено дальнейшее *контролируемое* хранение этого фрагмента. Формат сериализации сообщений продумайте самостоятельно.

Опционально: реализовать этап развёртывания серверного приложения на основе абстракции инверсии управления (IoC), реализованной в виде механизма внедрения зависимости (DI). Конфигурирование этапа развёртывания обеспечьте при помощи конфигурационных файлов и их трансформаций.

Опционально: обеспечить возможность репликации хранящихся в брокере сообщений данных.

4. Реализовать приложение (оконное или web), позволяющее:

- Инициировать выполнение протокола на создание секретного чата с указанием используемого симметричного алгоритма шифрования;
- Инициировать выполнение протокола на подключение к ранее созданному секретному чату;
- Инициировать выполнение протокола на отключение от секретного чата, к которому в данный момент существует подключение;
- Генерировать вектор инициализации (IV) для его применения в режимах шифрования: CBC, PCBC, CFB, OFB, CTR, Random Delta;
- Организовать функционал для выбора данных, подвергаемых шифрованию и передаче второй стороне, участвующей в секретном чате:
    - ввод текста в текстовое поле
    - выбор файла с данными при помощи стандартного диалога выбора файла
- Многопоточно (по возможности) шифровать данные сеансовым ключом симметричного алгоритма (с использованием одного из режимов шифрования: ECB, CBC, PCBC, CFB, OFB, CTR, Random Delta; также с использованием режима набивки: Zeros, ANSI X.923, PKCS7, ISO 10126);
- Инициировать выполнение протокола передачи вычисленного шифротекста на сторону серверного приложения при помощи нажатия кнопки на UI;
- Инициировать выполнение протокола получения шифротекста со стороны серверного приложения в фоновом режиме;
- Многопоточно (по возможности) дешифровать полученный шифротекст распределённым между сторонами сеансовым ключом симметричного алгоритма (с учётом режима шифрования и режима набивки, применённых при операции шифрования);
- Отображать список активных секретных чатов текущего пользователя;
- Отображать переданные и полученные сообщения в надлежащем виде (текст как текст, картинки как картинки, остальные файлы - как компоненты UI, позволяющие сохранить файлы на локальное устройство при помощи стандартного диалога сохранения файла;
- Сохранять переданные и полученные сообщения в локальной СУБД, устройство и взаимодействие с которой определите самостоятельно;
- Отображать прогресс операций шифрования / дешифрования / передачи данных / получения данных при помощи элементов управления типа ProgressBar;
- Инициировать отмену операции шифрования / дешифрования / передачи данных / получения данных по запросу пользователя;
- Инициировать выполнение протокола на отключение одного или обоих клиентов от секретного чата.

Приложение должно иметь интуитивно понятный и удобный пользовательский интерфейс. Поведение клиентского приложения, приводящее к аварийной ситуации, не допускается.

Для получения положительной (3 и выше) оценки за курсовой проект необходимо подготовить и сдать на кафедру респечатанную пояснительную записку. В пояснительной записке необходимо:

- описать реализованные алгоритмы шифрования и протоколы с теоретической точки зрения
- описать архитектуру своего комплекса приложений
- описать использованные средства использованных языков программирования и применённых при разработке технологий

Структура пояснительной записки:

- Титульный лист
- Содержание
- Введение
- Теоретическая часть (описание алгоритмов шифрования и протоколов)
- Практическая часть (описание архитектуры комплекса приложений, использованных языков программирования и применённых при разработке технологий)
- Вывод
- Список использованных источников
- Приложения (исходный код реализаций протокола Диффи-Хеллмана и алгоритмов шифрования по варианту)

Оформление пояснительной записки:

- Поля: левое 20мм, остальные 15мм
- Нумерация страниц: начиная с титульного листа, индексация инкрементальная начиная с 1; на титульном листе номер страницы не указывается
- Заголовки и подзаголовки разделов: шрифт Times New Roman 16pt, междустрочный интервал 1.5pt, выравнивание по левому краю
- Основной текст: шрифт Times New Roman 14pt, междустрочный интервал 1.15pt, выравнивание по ширине; абзацные отступы
- Рисунки: выравнивание по центру; под рисунком должна находиться подпись в формате

  Рисунок #. <Описание рисунка>

  , где # - номер рисунка при сквозной нумерации рисунков по всей пояснительной записке, индексация инкрементальная начиная с 1. Оформление подписи к рисунку: шрифт Times New Roman 12pt, курсивный, междустрочный интервал 1pt, выравнивание по центру; рисунок и подпись к нему должны находиться на одной странице пояснительной записки
- Таблицы: Выравнивание по центру; над таблицей должна находиться подпись в формате

  Таблица #. <Описание таблицы>

  , где # - номер таблицы при сквозной нумерации таблиц по всей пояснительной записке, индексация инкрементальная начиная с 1. Оформление подписи к таблице: шрифт Times New Roman 12pt, курсивный, междустрочный интервал 1pt, выравнивание по левому краю; таблица и подпись к ней должны находиться на одной странице пояснительной записки

- Листинги: Шрифт Consolas 12pt, междустрочный интервал 1pt, выравнивание по левому краю; над листингом должна находиться подпись в формате

  Листинг #. <Описание листинга>

  , где # - номер листинга при сквозной нумерации листингов по всей пояснительной записке, индексация инкрементальная начиная с 1. Оформление подписи к листингу: шрифт Times New Roman 12pt, курсивный, междустрочный интервал 1pt, выравнивание по левому краю; листинг и подпись к нему должны находиться на одной странице пояснительной записки
- Список использованных источников: оформление по ГОСТ 7.0.100-2018

Во время защиты курсового проекта необходимо уметь ориентироваться в коде, демонстрировать работу реализованного комплекса приложений, быть готовым отвечать на вопросы по использованным языкам программирования, технологиям, алгоритмам шифрования, протоколам взаимодействия и криптографическим протоколам.
Защита курсового проекта без распечатанной пояснительной записки не проводится.

Приложение 1. Варианты симметричных алгоритмов, реализуемых в курсовом проекте.

1 - Camellia, LOKI97
2 - Camellia, MacGuffin
3 - Camellia, MAGENTA
4 - Camellia, MARS
5 - Camellia, RC5
6 - Camellia, RC6
7 - Camellia, Serpent
8 - Camellia, Twofish
9 - LOKI97, MacGuffin
10 - LOKI97, MAGENTA
11 - LOKI97, MARS
12 - LOKI97, RC5
13 - LOKI97, RC6
14 - LOKI97, Serpent
15 - LOKI97, Twofish
16 - MacGuffin, MAGENTA
17 - MacGuffin, MARS
18 - MacGuffin, RC5
19 - MacGuffin, RC6
20 - MacGuffin, Serpent
21 - MacGuffin, Twofish
22 - MAGENTA, MARS
23 - MAGENTA, RC5
24 - MAGENTA, RC6
25 - MAGENTA, Serpent
26 - MAGENTA, Twofish
27 - MARS, RC5
28 - MARS, RC6
29 - MARS, Serpent
30 - MARS, Twofish
31 - RC5, RC6
32 - RC5, Serpent
33 - RC5, Twofish
34 - RC6, Serpent
35 - RC6, Twofish
36 - Serpent, Twofish

Приложение 2. Ссылка на документ с распределением вариантов симметричных алгоритмов, реализуемых в курсовом проекте.

https://docs.google.com/spreadsheets/d/1hT6-Y-TMp6d6cJeMxs_Js7C1gzFhmOljJJ3WSedVkjs/edit#gid=0