**Лабораторная работа 2.**

Написать программу «Защищенный блокнот» реализующую шифрование и просмотр зашифрованных текстовых файлов алгоритмом AES, Serpent или IDEA. Сервер и клиент должны быть на разных компьютерах. Лабораторную можно делать в паре без снижения.

**Минимальные требования(5 баллов)**

1. Серверная часть программы:
   1. хранит текстовые файлы,
   2. генерирует случайный сеансовый ключ по запросу клиента
   3. отправляет клиенту зашифрованный открытым ключом RSA сеансовый ключ.
   4. отправляет клиенту зашифрованный сеансовым ключом текстовый файл
2. Клиентская часть программы:
   1. Генерирует и отправляет серверу открытый ключ RSA (единожды).
   2. Отправляет серверу запрос с именем файла.
   3. Расшифровывает сеансовый ключ при помощи закрытого ключа RSA.
   4. Расшифровывает и отображает текстовый документ при помощи сеансового ключа.
   5. Ключ RSA сохраняется (генерируется по нажатию кнопки). Придумать свой метод хранения закрытого ключа.

**7 баллов**

1. В рамках одной сессии добавить возможность создавать, удалять и редактировать файлы. (Соединение шифруется одним ключом)

**8-9 баллов**

1. Добавить поддержку многих пользователей.
2. Добавить в программу аутентификацию по паролю.
3. Использовать вместо RSA ECDSA или GM алгоритмы.
4. Добавить срок годности к сеансовому ключу.

**10 баллов**

1. Защитить данные на сервере от взломщика, у которого есть доступ к хранилищу.
2. Продемонстрировать атаку man-in-the-middle для вашей системы.

**Варианты**

1. AES, режим сцепления блоков (СВС — Cipher Block Chaining)
2. AES, режим обратной связи по шифротексту (CFB — Cipher Feed Back)
3. AES, режим обратной связи по выходу (OFB — Output Feed Back)
4. Serpent, режим сцепления блоков (СВС — Cipher Block Chaining)
5. Serpent, режим обратной связи по шифротексту (CFB — Cipher Feed Back)
6. Serpent, режим обратной связи по выходу (OFB — Output Feed Back)
7. IDEA, режим сцепления блоков (СВС — Cipher Block Chaining)
8. IDEA, режим обратной связи по шифротексту (CFB — Cipher Feed Back)
9. IDEA, режим обратной связи по выходу (OFB — Output Feed Back)