Лабораторная работа 2.

Написать программу «Защищенный блокнот» реализующую шифрование и просмотр зашифрованных текстовых файлов алгоритмом AES, Serpent или IDEA.

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

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

Дополнительные задания:

1) Добавить в программу аутентификацию по паролю
2) Использовать вместо RSA алгоритм GM либо схему ECIES(с алгоритмом шифрования согласно варианту)
3) Добавить срок годности к сеансовому ключу
4) Реализовать клиент на платформе Android