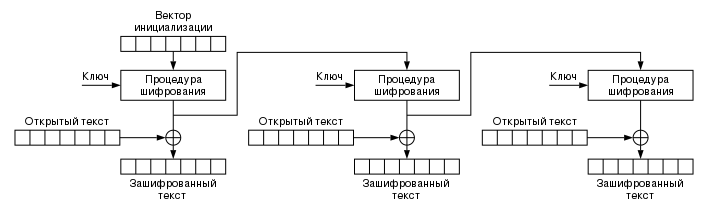
**КБРС. Лабораторная работа №4 (а также включает 2-ую)  
Харченко Роман**

Вариант 9: IDEA, режим обратной связи по выходу (OFB)

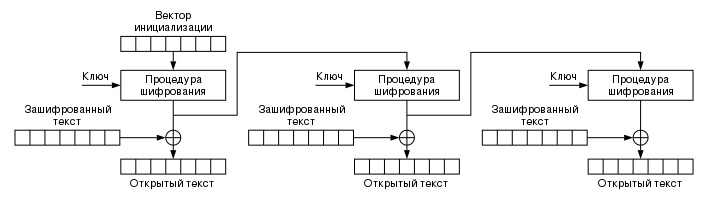
Также были реализованы:

1. Аутентификация по паролю
2. Срок годности сеансового ключа
3. Использовал GM алгоритм вместо RSA

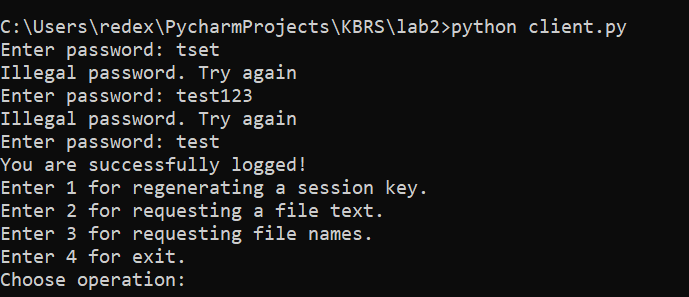
Шифрование OFB:



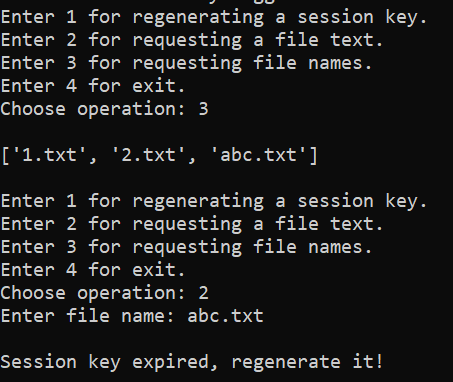
Дешифрование в OFB:



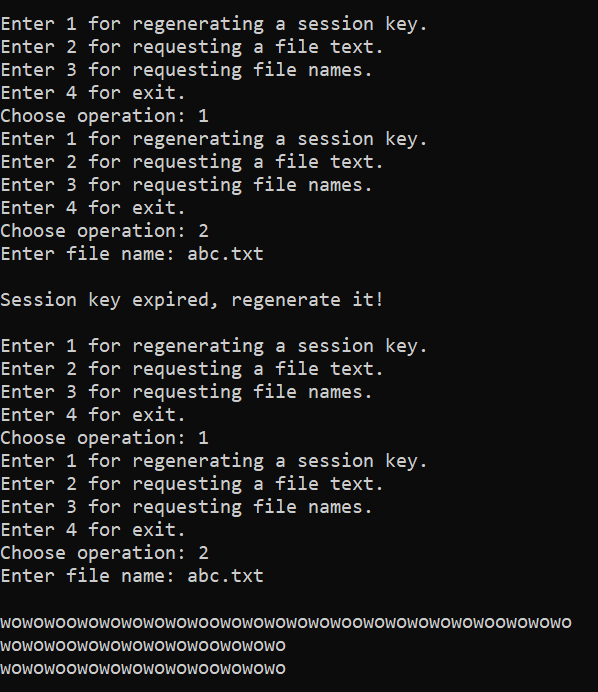
При подключении к серверу на клиенте нас встречает сообщение с просьбой ввести пароль:



Как видно из скриншота, как только мы успешно аутентифицировались, нас встречает меню сервера, давайте попробуем запросить названия файлов, а затем содержание этого файла, но не будем генерировать сессионный ключ.



Как можно заметить, нас просят сначала сгенерировать ключ.



Сначала мы попробовали сгенерировать ключ и запросить содержимое файла спустя 10 секунд, но нам написало, что ключ уже не валиден. Это связано с тем, что я сделал время жизни ключа в 10 секунд. А во втором случае 10 секунд не прошло и содержимое вернулось успешно.

Для того, чтобы аутентифицироваться в системе используется стандартный способ: ввод логина и пароля. Если указанный логин и пароль соответствует тем, которые записаны в базу данных, то будет происходить вход в систему. При этом также согласно варианту будет генерироваться токен, который создаётся на время сессии входа, можно также указать время, на время которого будет действовать данный токен, а по его истечению удалится, таким образом будет обеспечена дополнительная защита, так как злоумышленник не сможет постоянно пользоваться Вашим аккаунтом. В результате получается 2-факторная авторизация.

В результате чего получается, что пользователь при получении доступа к аккаунту также ещё получит и персонализированный токен, таким образом, это позволит избежать нежелательного доступа со стороны злоумышленника, так как токен постоянно выдаётся новый и действует он лишь какой-то заданный промежуток времени.