Задание к курсовой работе по основам криптографии.

1. Реализовать асимметричный алгоритм шифрования.
2. Реализовать симметричный алгоритм шифрования.
3. Реализовать приложение (оконное или web), позволяющее:
   - Генерировать сеансовый ключ симметричного алгоритма;
   - Генерировать ключи асимметричного алгоритма в целях распределения между сторонами, участвующими в обмене данными, сеансового ключа (простые числа, требуемые при генерации ключей, должны иметь в битовом представлении размер не менее 64 бит и должны генерироваться вероятностными тестами простоты (Соловея-Штрассена, Миллера-Рабина, Ферма));
   - Генерировать вектор инициализации (IV) для его применения в режимах шифрования: CBC, CFB, OFB, CTR, RD, RD+H;
   - Асинхронно и многопоточно (по возможности) шифровать файл распределённым между сторонами сеансовым ключом (с использованием IV при режиме шифрования, отличном от ECB) на одной стороне с последующей передачей ею зашифрованного файла (вместе с вектором инициализации) другой стороне;
   - Асинхронно и многопоточно (по возможности) дешифровать переданный зашифрованный файл распределённым между сторонами сеансовым ключом (с использованием IV при режиме шифрования, отличном от ECB), с избавлением от набивки (padding);
   - Отображать прогресс операций шифрования и дешифрования при помощи элемента управления ProgressBar;
   - Опционально: отменить операцию [де]шифрования/скачивания/загрузки по запросу пользователя.

Передача файлов должна быть организована при помощи сервера, на который можно отправить зашифрованный файл и скачать его. На/С сервер(а) одновременно можно отправлять/скачивать произвольное количество файлов. Структура файлов произвольна (текст, изображения, видео, аудио, etc.). Количество клиентских приложений, подключаемых к серверному, произвольно. Для симметричного алгоритма используйте тип набивки (padding) PKCS7.

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

- описать архитектуру своего комплекса приложений
- описать использованные средства использованных языков программирования и технологий
- привести полный исходный код реализованного комплекса приложений

Во время защиты курсовой работы необходимо уметь ориентироваться в коде, демонстрировать работу реализованного комплекса приложений, быть готовым отвечать на вопросы по использованным языкам программирования, технологиям, алгоритмам шифрования.

Варианты курсовой работы:

1 - ElGamal + RC6
2 - NTRUEncrypt + RC6
3 - LUC + RC6
4 - Benaloh + RC6
5 - XTR + RC6
6 - ElGamal + SHACAL-1
7 - NTRUEncrypt + SHACAL-1
8 - LUC + SHACAL-1
9 - Benaloh + SHACAL-1
10 - XTR + SHACAL-1
11 - ElGamal + DEAL
12 - NTRUEncrypt + DEAL
13 - LUC + DEAL
14 - Benaloh + DEAL
15 - XTR + DEAL
16 - ElGamal + MARS
17 - NTRUEncrypt + MARS
18 - LUC + MARS
19 - Benaloh + MARS
20 - XTR + MARS
21 - ElGamal + Twofish
22 - NTRUEncrypt + Twofish
23 - LUC + Twofish
24 - Benaloh + Twofish
25 - XTR + Twofish
26 - ElGamal + Serpent
27 - NTRUEncrypt + Serpent
28 - LUC + Serpent
29 - Benaloh + Serpent
30 - XTR + Serpent
31 - ElGamal + Camellia
32 - NTRUEncrypt + Camellia
33 - LUC + Camellia
34 - Benaloh + Camellia
35 - XTR + Camellia
36 - ElGamal + MAGENTA
37 - NTRUEncrypt + MAGENTA
38 - LUC + MAGENTA
39 - Benaloh + MAGENTA
40 - XTR + MAGENTA
41 - ElGamal + Blowfish
42 - NTRUEncrypt + Blowfish
43 - ElGamal + Blowfish