Задание к курсовой работе по основам криптографии.

1. Реализовать симметричный алгоритм шифрования.
2. Реализовать асимметричный 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 (если возможно) шифровать файл распределённым 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 (если возможно) дешифровать переданный зашифрованный файл распределённым 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/передачи/ скачивания 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. Для симметричного алгоритма используйте тип набивки (padding) PKCS7.

Варианты:

Артов	ElGamal, RC6	Алимов	LUC, Blowfish
Байтякова	LUC, SHACAL	Буреева	LUC, DEAL
Вартумян	ElGamal, MAGENTA	Денисова	Benalo, SAFER
Верховский	Benalo, MAGENTA	Евкарпиев	ElGamal, Serpent
Гапшенко	LUC, RC6	Заиц	Benalo, LOKI97
Жаворонков	Benalo, Blowfish	Ложкина	Benalo, SHACAL
Зеленер	NTRUEncrypt, DEAL	Лысаковская	ElGamal, E2
Карначёв	LUC, Serpent	Мамченков	Benalo, FROG
Кирьянов	Benalo, E2	Петрова	NTRUEncrypt, FROG
Лебедева	NTRUEncrypt, Blowfish	Сергеев	NTRUEncrypt, LOKI97
Муханов	NTRUEncrypt, SHACAL	Солдатов	ElGamal, Camellia
Нестеров	LUC, MAGENTA	Сорокин	NTRUEncrypt, HPC
Познанский	Benalo, Camellia	Терешков	LUC, FROG
Семёшкин	NTRUEncrypt, Serpent	Тришин	Benalo, RC6
Смирнов	Benalo, MARS	Унжаков	ElGamal, LOKI97
Таскина	Benalo, Twofish	Чернова	ElGamal, Blowfish
Цыкина	NTRUEncrypt, E2	Шадай	NTRUEncrypt, MAGENTA
Шекунов	ElGamal, SHACAL	Янковский	ElGamal, Twofish
Юрьев	NTRUEncrypt, Camellia		