

***Тема “Криптографические протоколы”***

***Общее задание на программирование на любом языке***, те. решение заданий из 3-х файлов с использованием ЯП

Требуется разработать ***клиент-серверное приложение***, которое должно позволять зашифровывать или расшифровать выбранный файл указанным (выбирается пользователем из списка) криптографическим протоколом.

К приложению предъявляются следующие требования:

1. Клиент-серверное приложение для управления вычислительным процессом должно состоять из двух частей: клиент и сервер, которые должны образовывать единую распределенную вычислительную систему.

2. Серверное приложение должно обеспечивать подключение нескольких клиентов одновременно.

3. Клиентское приложение должно обеспечивать подключение к серверу.

4. Серверное приложение должно иметь интуитивно понятный графический интерфейс.

5. В окне серверного приложения должна быть возможность выбора файла для зашифрования/расшифрования, криптографического протокола, пути, по которому необходимо сохранить результирующий файл (если это нужно). Также, во время выполнения работы с приложением, должен отображаться прогресс решения задачи.

6. Клиентское приложение может быть как консольным, так и Desktop. В окне приложения должна выводиться минимальная информация о ходе выполнения работы.

7. Клиентское приложение должно распараллелить обработку полученной порции информации для достижения большей производительности. Распараллеливание работы должно выполняться через разделение полученной порции информации на более мелкие блоки и обработка их в отдельных нитях.

8. Кластер должен выполнять шифрование файла согласно заданному криптографическому протоколу.

9. Обмен данными между клиентом и сервером должен выполняться с использованием протокола TCP/IP.

10. Клиентское и серверное приложение необходимо разбить на модули. Это повысит наглядность и легкость восприятия кода программы, а также облегчит поиск и исправление возможных ошибок.

11. Взаимодействие пользователя с приложением должно осуществляться с помощью клавиатуры и мыши.

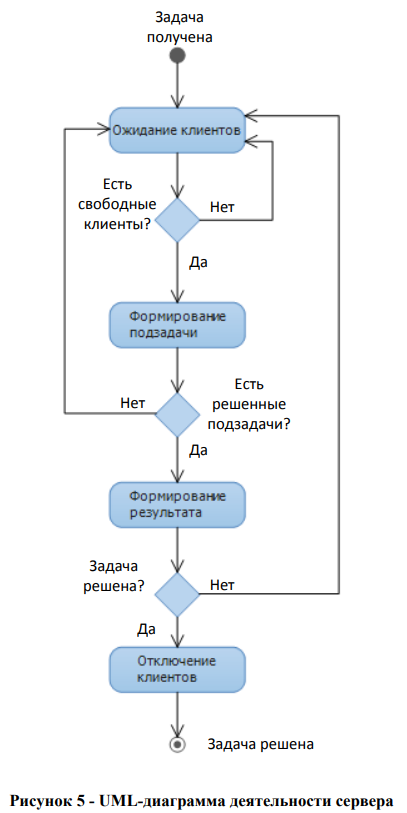
12. Операционная система – MS Windows 7/8/10.

 Итак, Вам необходимо разработать реализовать ***клиент-серверное*** приложение реализации алгоритмов различных криптографических протоколов (описание см. в текстах практических работ), в котором для клиента и для сервера реализованы следующие действия:

I. Реализовать ***клиент-серверное*** приложение реализации алгоритмов различных криптографических протоколов (описание см. в текстах практических работ), позволяющее выполнять следующие действия:   
1. Шифровать открытые данные (на стороне клиента) по описанному в тексте алгоритму или выполнять перераспределение ключей для шифрования (см. описание алгоритма):  
1) шифруемый текст должен храниться в одном файле, а ключ зашифрования – в другом;  
2) зашифрованный текст должен сохраняться в файл;  
3) в процессе шифрования предусмотреть возможность выбора криптографического протокола, просмотра и изменения ключа, шифруемого и зашифрованного текстов в шестнадцатеричном и в символьном виде;  
4) приложение должно показывать время шифрования и время пересылки.  
II. Реализовать ***клиент-серверное*** приложение для расшифрования, позволяющее выполнять следующие действия:  
1. Расшифровать данные (на стороне другого клиента) по описанному в тексте алгоритму:  
1) зашифрованный текст должен храниться в одном файле, ключ – в другом;  
2) расшифрованный текст должен сохраняться в файл;  
3) в процессе расшифрования предусмотреть возможность выбора криптографического протокола, просмотра и изменения ключа, зашифрованного и расшифрованного текстов в шестнадцатеричном и символьном виде;

4) приложение должно показывать время шифрования и время пересылки.

III. Реализовать ***серверное*** приложение для связи двух клиентов.



*Срок сдачи - 1 месяц.*

*За все задания из 3-х файлов - 30 баллов.*