Лабораторная работа №2
СТБ 34.101.66

Дедлайн: 08.12.2025

1 Введение

В данной лабораторной работе вам необходимо реализовать приложение, с помощью которого два клиента (Алиса и Боб) смогут произвести **взаимную** аутентификацию, сформировать общий ключ и на его основе организовать защищенный канал передачи данных.

2 Условие лабораторной работы

Основная часть (20 баллов)

Реализовать определенный в СТБ 34.101.66 криптографический протокол формирования общего ключа для уровня стойкости $l = 128$:

1. BMQV (СТБ 34.101.66, п. 7.4);
2. BSTS (СТБ 34.101.66, п. 7.5);
3. BPACE (СТБ 34.101.66, п. 7.6);

Предполагается, что абоненты и Трент (при его наличии) имеют заранее сгенерированные в соответствии с алгоритмом генерации пары ключей (СТБ 34.101.45, п. 6.2.2) долговременные личный и открытый ключи, которые хранятся в виде отдельных файлов.

Если протокол подразумевает использование сертификата (BMQV, BPACE), то для открытых ключей абонентов должны быть выпущены мини-сертификаты в виде тройки элементов (имя абонента, открытый ключ абонента, подпись Трента), при этом Трент вырабатывает подпись от конкатенации строки с именем абонента и строки с его открытым ключом. Для проверки подписи Трента необходимо использовать открытый ключ Трента явно заданный в исходной коде вашей программы. Для протокола BPACE предполагается, что оба абонента знают заранее распределенный пароль.

Выбор номера протокола для реализации из списка выше следует выполнять по формуле $N \ mod \ 3 + 1$, где N — ваш номер в списке группы (можно увидеть тут).

Обратите внимание, что необязательные шаги протокола (они обозначены квадратными скобками) являются обязательными для реализации в рамках данной лабораторной работы.

Дополнительная часть (15 баллов)

Реализовать определенный в СТБ 34.101.79 криптографический протокол организации защищенного соединения (СТБ 34.101.79, п. 8.5), используя в качестве ключа K_0 сформированный в рамках реализованного ранее протокола формирования общего ключа.

Предполагается, что абоненты передают по защищенному соединения текстовые строки, длина которых не превосходит 256 байт.

Бонусная часть (от 5 до 15 баллов)

Дополнительно баллы можно получить за:

- реализацию абонентов в виде отдельных программ, а не различных функций, вызываемых в рамках одной программы;
- графический интерфейс программы;
- парольную защиту долговременных личных ключей абонентов при хранении;
- использование совокупности системных и биологических источников энтропии для формирования сеансовых ключей;
- возможность передачи по защищенному соединению больших файлов;
- другие модификации программы по согласованию с преподавателем.

Особенности реализации лабораторной работы

- Под реализацией следует понимать программу, написанную на одном из языков программирования: C, C++, C#, Java, Python, Go.

- Программа должна выводить весь процесс установления соединения и обмена информацией по защищенному соединению на экран и/или в файл. Это значит, что для каждого шага протокола формирования общего ключа, а также алгоритмов установки и снятия защиты в шестнадцатеричном виде должны выводиться все ключи и другие криптографические объекты.

- Допускается использование любого стандартного источника случайности, который присутствует в выбранном языке программирования.

- Разрешается не реализовывать используемые в рамках протоколов формирования общего ключа и организации защищенного соединения криптографические алгоритмы самостоятельно, а подключить их реализацию из криптографической библиотеки с открытым исходным кодом Bee2 или криптографической библиотеки с закрытым исходным кодом TZICrypt.

3 Порядок сдачи лабораторной работы

- Вам необходимо создать архив формата «.zip», название которого должно иметь вид «Ivanov_2.zip», где «Ivanov» – ваша фамилия латинскими буквами. В архиве должен быть исходный код вашей реализации.

- Не позже, чем за 24 часа до сдачи лабораторной работы преподавателю, вы должны отправить архив по одному из контактов, указанных в ответе на вопрос №3 в файле «FAQ.pdf».