1. Министерство науки и высшего образования Российской Федерации
2. Санкт-Петербургский политехнический университет Петра Великого
3. Институт компьютерных наук и кибербезопасности
4. Высшая школа кибербезопасности

**ОТЧЕТ**

**ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5**

1. **«Криптосистемы на основе задачи дискретного логарифмирования»**
2. по дисциплине «Криптографические методы защиты информации»
3. Выполнил:
4. студент гр. 5151001/00201 А.А. Устюгов

<*подпись*>

1. Проверил
2. старший преподаватель, к.т.н А.В. Тулинова

<*подпись*>

1. Санкт-Петербург

2024

1. **СОДЕРЖАНИЕ**

[1 Формулировка задания 3](#_Toc165639282)

[2 Ход работы 4](#_Toc165639283)

[3 Тестирование 5](#_Toc165639284)

[4 Контрольные вопросы 9](#_Toc165639285)

[5 Выводы 11](#_Toc165639286)

# Формулировка задания

Цель работы – изучение протоколов шифрования с открытым ключом и электронной подписи, безопасность которых основана на задаче дискретного логарифмирования в конечном поле.

Задачи – разработать программу, которая, в соответствии с вариантом, реализует одну из криптосистем на основе задачи дискретного логарифмирования.

Вариант – 6.

# Ход работы

Протокол Месси–Омуры требует диалога между отправителем и получателем и, следовательно, для его реализации необходим двунаправленный канал связи. В качестве канала связи используются сокеты.

Бесключевое шифрование Месси–Омуры

*Вход отправителя и получателя*. Циклическая группа 𝐺 большого простого порядка *r*, вычислимая в обе стороны функция 𝑓: 𝑀→𝐺.

*Результат*. Зашифрование и расшифрование сообщения 𝑚.

1. Отправитель вычисляет 𝑡←𝑓(𝑚) для сообщения 𝑚. Если 𝑡 является единичным элементом 𝑒 группы 𝐺, то результат: сообщение зашифрованию не подлежит.

2. Отправитель генерирует случайный показатель 𝑎∈𝔽𝑟∗, вычисляет элемент 𝑡𝑎 группы 𝐺 и направляет элемент 𝑡𝑎 получателю.

3. Получатель вырабатывает случайный показатель 𝑏, обратимый по модулю *r*, вычисляет (𝑡𝑎)𝑏=𝑡𝑎𝑏 и посылает элемент 𝑡𝑎𝑏 отправителю.

4. Отправитель возводит полученный элемент в степень 𝑎−1(𝑚𝑜𝑑𝑟): (𝑡𝑎𝑏)𝑎−1=𝑡𝑏 и посылает 𝑡𝑏 получателю.

5. Получатель возводит полученный элемент в степень 𝑏−1(𝑚𝑜𝑑𝑟): (𝑡𝑏)𝑏−1=𝑡 и вычисляет 𝑚←𝑓−1(𝑡).

В качестве группы G была взята группа точек эллиптической кривой, в качестве сообщения ключ AES.

Сообщения вкладываю в точку следующим способом: дополняю ключ 1 байтом, и перевожу ключ в десятичное представление – это x-координата точки. Если из правой части уравнения кривой можно взять корень, то точка найдена, если нет, то добавляю к x единицу. Если пришлось добавить больше 255 раз, то вернуть ошибку.

Для генерации кривой с необходимыми параметрами использовался скрипт, написанный с помощью SageMath.

# Тестирование

Параметры криптосистемы представлены на рисунке 1.

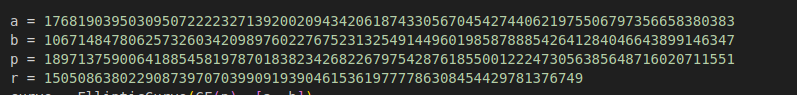


Рисунок 1 – параметры криптосистемы

В результате обмена сообщениями устанавливается симметричный ключ шифрования (рисунок 2).

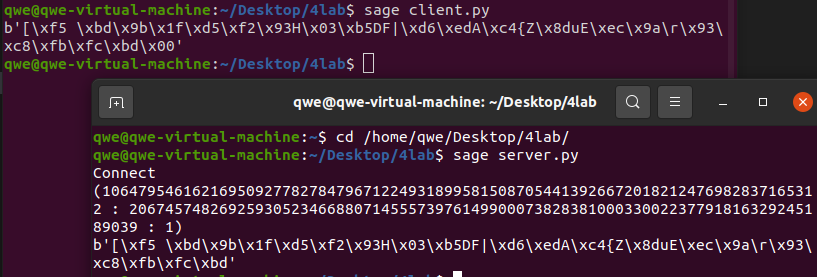


Рисунок 2 – ключ на клиенте и сервере

На рисунках 3, 4, 5 представлены asn1 форматы передаваемых сообщений.

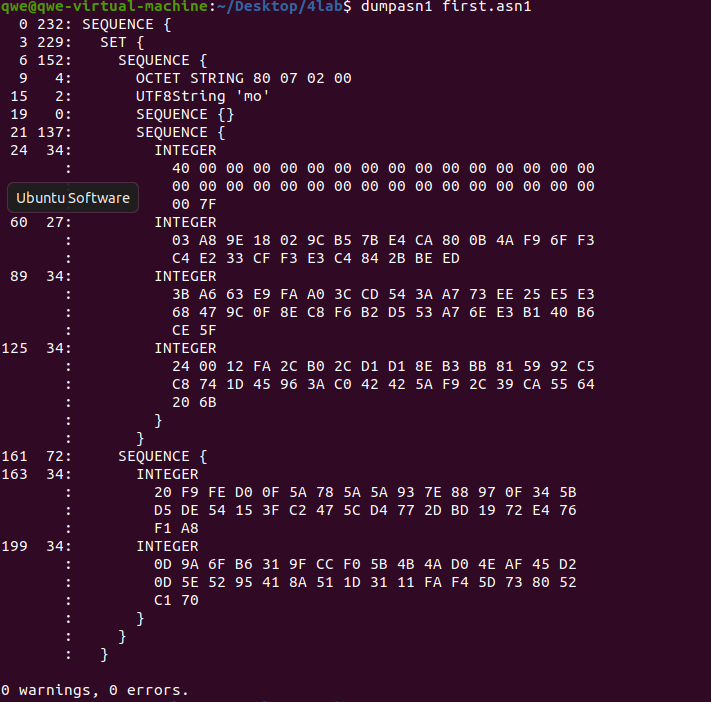


Рисунок 3 – сообщение от клиента к серверу с передачей параметров криптосистемы и точки aP

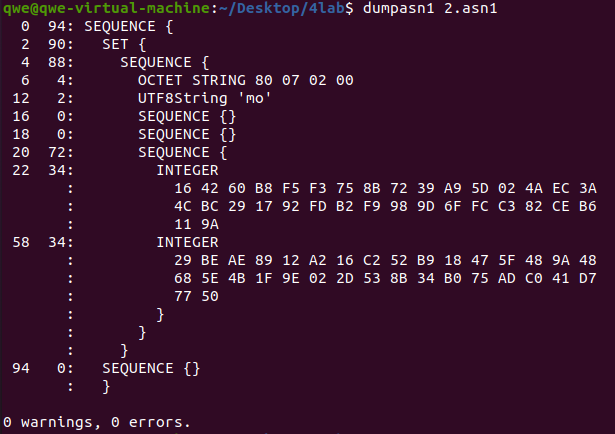


Рисунок 4 – сообщение от сервера к клиенту с передачей точки abP

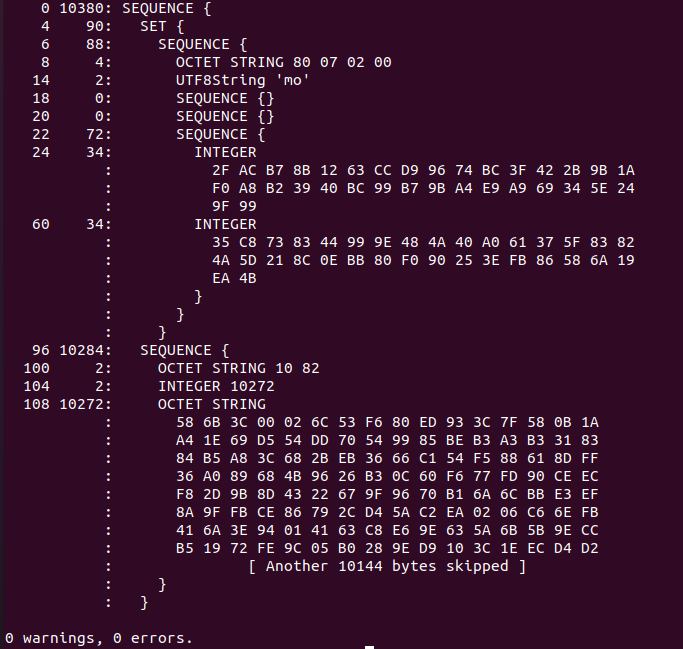


Рисунок 5 – сообщение от клиента к серверу с передачей точки bP и зашифрованным сообщением.

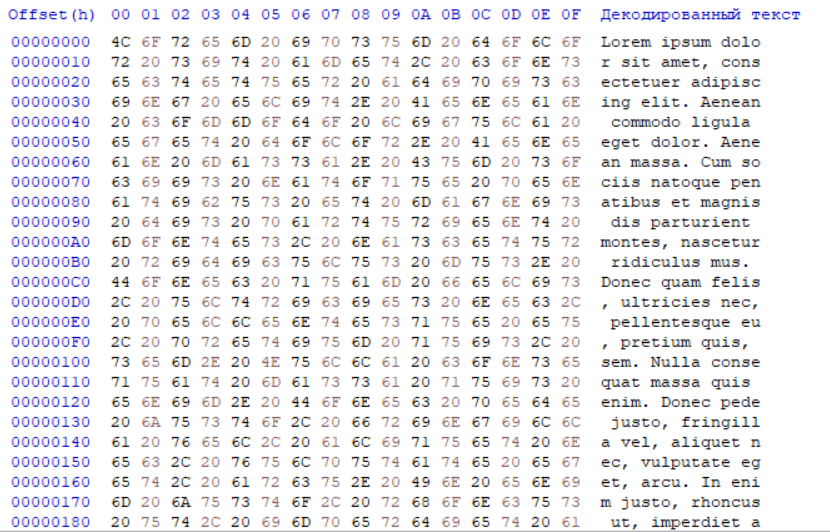


Рисунок 6 – сообщение для передачи в открытом виде

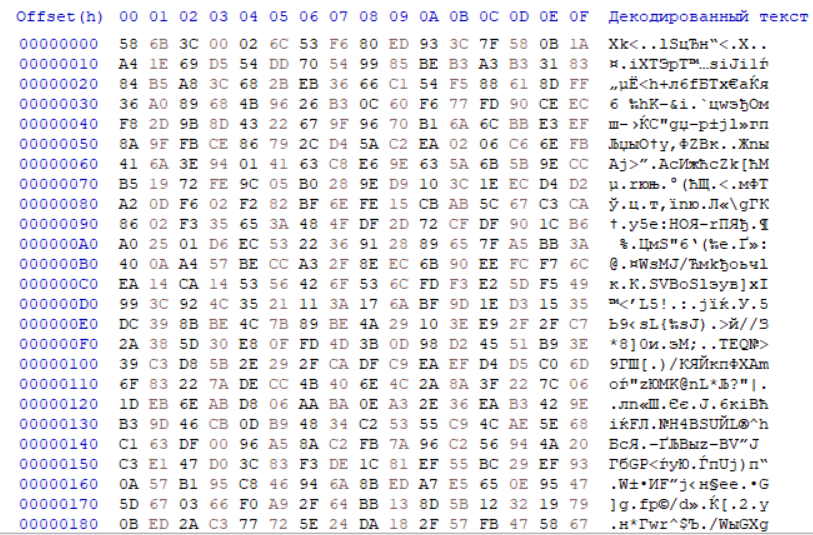


Рисунок 7 – зашифрованное сообщение

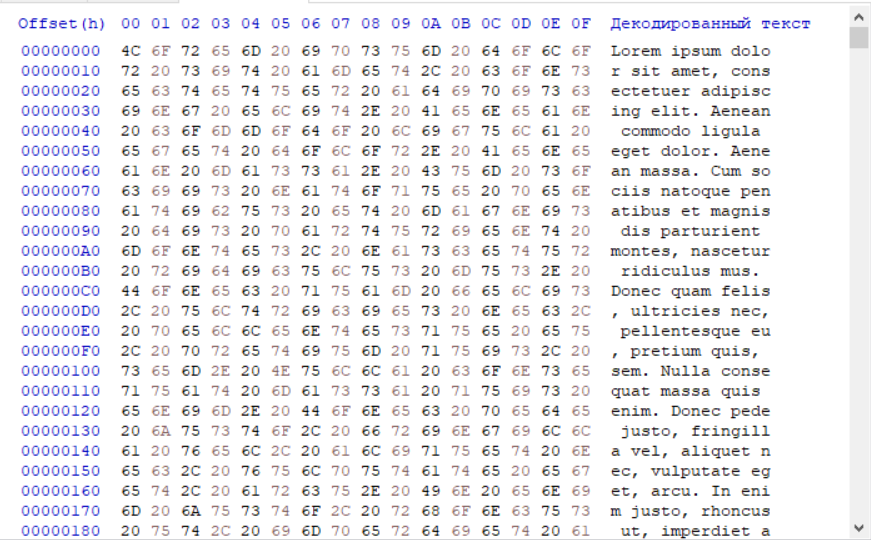


Рисунок 8 – расшифрованное сервером сообщение

# Контрольные вопросы

1. Пусть 𝐺 – конечная циклическая группа с заданной образующей. Порядок группы 𝐺 известен и делится на простое число 𝑟. Как найти образующую циклической подгруппы порядка 𝑟?

Пусть порядок G равен p. Тогда , следовательно, т.к. p:r, , соответственно, элемент является образующим элементом подгруппы порядка r.

2. Покажите, что задача Месси–Омуры сводится к задаче дискретного логарифмирования.

Даны ta, tb, tab. Они известны всем и передаются по открытому каналу. Пусть . Найдя a, можно найти t, a находится как решение задачи дискретного логарифмирования.

3. Подвержен ли протокол шифрования Эль-Гамаля к атаке на основе подобранных шифртекстов?

Подвержен. Предположим, что наш шифртекст

Тогда посчитаем и отправим его оракулу расшифрования. , . Тогда при расшифровки мы получим . Для того, чтобы получить , необходимо домножить на .

1. Перечислите задачи, положенные в основу схемы подписи Эль-Гамаля. Почему важно, чтобы период генератора случайных чисел, используемого в схеме подписи, был достаточно большим?

В основу схемы подписи Эль-Гамаля положены задачи дискретного логарифмирования и задача предсказания случайного числа. Если период генератора будет маленьким, можно отследить случайное число k, а зная его можно вычислить и ключ x.

# Выводы

В ходе выполнения лабораторной работы были изучены протоколы, основанные на задаче дискретного логарифмирования - протоколы Эль-Гамаля, Диффи-Хеллмана и Месси-Омуры. Был реализован протокол Месси-Омуры. Возможными уязвимостями в реализации является то, что по итогу точки были не из простой подгруппы, соответственно нарушитель может извлечь некоторую информацию об открытом тексте, вычислив для шифртекста характер степени . Также протокол Месси-Омуры уязвим к атаке «человек по середине». Необходимо дополнительно подписывать отправляемые сообщения, чего в моей программе сделано не было.