# лабораторная работа №4 “Атака MITM”

## Цель работы

Целью работы является знакомство с классическим видом атаки на криптографические системы «человек посередине» (man-in-the-middle).

## Основные сведения

**Человек посередине**

Атака посредника, атака «человек посередине», MITM-атака (англ. Man in the middle) — термин в криптографии, обозначающий ситуацию, когда криптоаналитик (атакующий) способен читать и видоизменять по своей воле сообщения, которыми обмениваются корреспонденты, причём ни один из последних не может догадаться о его присутствии в канале.

Метод компрометации канала связи, при котором взломщик, подключившись к каналу между контрагентами, осуществляет вмешательство в протокол передачи, удаляя или искажая информацию.

**Принцип атаки**

Атака обычно начинается с прослушивания канала связи и заканчивается тем, что криптоаналитик пытается подменить перехваченное сообщение, извлечь из него полезную информацию, перенаправить его на какой-нибудь внешний ресурс.

**Пример атаки**

Атака «человек посередине».

Предположим, что Алиса хочет передать Бобу некоторую информацию. Мэлори хочет перехватить сообщение и, возможно, изменить его так, что Боб получит неверную информацию.

Мэлори начинает свою атаку с того, что устанавливает соединение с Бобом и Алисой, при этом они не могут догадаться о том, что кто-то третий присутствует в их канале связи. Все сообщения, которые посылают Боб и Алиса, приходят Мэлори.

Алиса просит у Боба его открытый ключ. Мэлори представляется Алисе Бобом и отправляет ей свой открытый ключ. Алиса, считая, что это ключ Боба, шифрует им сообщение и отправляет его Бобу. Мэлори получает сообщение, расшифровывает, затем изменяет его, если нужно, шифрует его открытым ключом Боба и отправляет его ему. Боб получает сообщение и думает, что оно пришло от Алисы:

Алиса отправляет Бобу сообщение, которое перехватывает Мэлори:

Алиса «Привет Боб, Это Алиса. Пришли мне свой открытый ключ» → Мэлори Боб

Мэлори пересылает сообщение Бобу; Боб не может догадаться, что это сообщение не от Алисы:

Алиса Мэлори «Привет Боб, Это Алиса. Пришли мне свой открытый ключ» → Боб

Боб посылает свой ключ:

Алиса Мэлори ← [ключ Боба] Боб

Мэлори подменяет ключ Боба своим и пересылает сообщение Алисе:

Алиса ← [ключ Мэлори] Мэлори Боб

Алиса шифрует сообщение ключом Мэлори, считая что это ключ Боба, и только он может расшифровать его:

Алиса «Встретимся на автобусной остановке!» [зашифровано ключом Мэлори] → Мэлори Боб

Мэлори расшифровывает сообщение, читает его, модифицирует его, шифрует ключом Боба и отправляет его:

Алиса Мэлори «Жди меня у входа в музей в 18:00!» [зашифровано ключом Боба] → Боб

Боб считает, что это сообщение Алисы.

Этот пример демонстрирует необходимость использования методов для подтверждения того, что обе стороны используют правильные открытые ключи, то есть что у стороны А открытый ключ стороны Б, а у стороны Б открытый ключ стороны А. В противном случае, канал может быть подвержен атаке «человек посередине».

Предположим, объект A планирует передать объекту B некую информацию. Объект C обладает знаниями о структуре и свойствах используемого метода передачи данных, а также о факте планируемой передачи собственно информации, которую С планирует перехватить. Для совершения атаки С «представляется» объекту А как В, а объекту В — как А. Объект А, ошибочно полагая, что он направляет информацию В, посылает её объекту С. Объект С, получив информацию, и совершив с ней некоторые действия (например, скопировав или модифицировав в своих целях) пересылает данные собственно получателю — В; объект В, в свою очередь, считает, что информация была получена им напрямую от А.

## Задание

Изучить принцип атаки «человек посередине». Выбрать криптосистему для демонстрации атаки. Разработать и реализовать все стороны обмена и продемонстрировать динамический перехват и подмену сообщений в криптосистеме. Оценить производительность методов атаки, степень применимости и эффективности по сравнению с другими видами атак на криптосистему.

## Порядок выполнения

1. Изучить принцип атаки «человек посередине».
2. Выбрать криптосистему для демонстрации атаки. Разработать и реализовать все стороны обмена.
3. Провести динамический перехват и подмену сообщений в криптосистеме.
4. Оценить производительность методов атаки, степень применимости и эффективности по сравнению с другими видами атак на криптосистему.

## Содержание отчета

1. Цель работы.
2. Задание.
3. Краткая теория.
4. Выдержки из текста программы, реализующие критичные для работы алгоритмов атаки участки.
5. Примеры работы сторон в криптосистеме, демонстрирующие перехват и подмену сообщений.
6. Выводы по работе.