Московский физико-технический институт

Эсее по защите информации

Криптографические протоколы. Протокол Girault.

Выполнила студентка Б01-907

Юлия Прохорова

Долгопрудный, 2022

Содержание

> Кто владеет информацией, тот владеет и миром.
>
> Натан Майер Ротшильд

1. Введение

Криптографию называют наукой или даже искусством безопасных сообщений. Криптография встречается и в повседневной жизни, например, можно зашифровать ваш личный дневник, чтобы никто другой не смог его прочитать. Но здесь мы поговорим о криптографии, которая защищает важные файлы, документы или банковские счета от любого, кто попытается их прочесть.

> Брюс Шнайер пишет: "Если я беру письмо, кладу его в сейф где-нибудь в Нью-Йорке, затем велю Вам прочитать это письмо, то это не безопасность. Это непонятно что. С другой стороны, если я беру письмо и кладу его в сейф, затем передаю этот сейф Вам вместе с детальным описанием, передаю также сотню подобных сейфов с их комбинациями, чтобы Вы и лучшие "медвежатники мира"могли изучить систему замков, а вы все равно не сможете открыть сейф и прочитать письмо - вот это и есть безопасноть."

Современная криптография - общирная область знаний, сложившаяся в результате серьезных исследований на протяжении последних десятков лет. Данная работа направлена на то, чтобы познакомить читателя с криптографическими протоколами, а именно с протоколом Girault. Но не обо всем сразу. Начнем с сновных понятий и терминов.

2. Общая теория

Обычная ситуация, которую рассматривают, когда изучают криптографию:

- есть две стороны: отправитель и получатель;
- первый хочет послать сообщение второму;
- при этом отправлять сообщение необходимо безопасным образом - чтобы любой перехвативший не смог его прочесть.

В данном случае само сообщение будет называться **открытым текстом**. Изменение сообщения так, чтобы не была понятна его суть - это **шифрование**, полученный текст - **шифротекст**. **Дешифрованием** же называется процесс преобразования шифротекста в открытый текст. **Шифр** представляет собой обратимую математическую функцию, используемая для шифрования и дешифрования.

Шифрование разделяют на две основные группы: **симметричные** и соответственно **ассиметричные**. Для обеих групп необходимо наличия ключа для шифрования и дешифрования, однако в разных группах реализация отличается. В случае симметричных шифров есть два варианта:

- обе операции используют один и тот же ключ K;
- ключ дешифрования K_2 можно получить из ключа шифрования K_1 простейшей операцией;

Группу симметричных шифров разделяют на:

- **блочные**
  - за одну операцию шифрования происходит преобразование одного блока данных;
  - размеры блоков одинаковы;
  - результат шифрования блока может зависеть от предыдущего;
- **потоковые**
  - работают с каждым символом открытого текста по-отдельности;

Вернемся к ассиметричным шифрам. Как читатель, вероятно, уже догадался - для таких шифров ключ для дешифрования K_2 получить из ключа шифрования K_1 сложно.

2.1. Протоколы

Протокол - порядок действий, предпринемаемых сторонами, чтобы решить поставленную задачу. Каждое действие должно выполняться в свою очередь и только после окончания предыдущего.

Каждый протокол должен обладать следующими характеристиками:

- **Известность** - каждый участник протокола должен знать протокол и последовательность составляющих его действий;
- **Согласованность** - каждый участник протокола должен согласиться следовать ему;
- **Отсутствие противоречий (прозрачность)** - каждое действие должно быть определено так, чтобы не было возможности непонимания;
- **Полнота** - каждой ситуации соответствует определенное заранее действие.

Используя криптографический протокол, участники протокола могут:

- безопасно передавать друг другу сообщения;
- делиться секретом друг с другом;
- случайно генерировать случайную последовательность;
- подтверждать свою подлинность;
- подписывать контракт одновременно.

Для демонстрации работы протоколов обычно определяют участников: Alice - начинает протокол, Bob - отвечает, также при необходимости дополнительных сторон появляются Carol и Dave.

Далее рассмотрим основные виды протоколов:

2.1.1. Протокол с посредником

Посредник - незаинтересованная 3я сторона, которая завершает протокол. Такой протокол используют, если стороны недоверяют друг другу. При этом все участники протокола принимают за истину все, что скажет посредник. Все его действия - правильные, и все стороны протокола уверены в том, что посредник выполнит свою часть протокола.

У данного протокола, как и любого другого существуют недостатки:

- сложно доверять безликому посреднику;
- компьютерная сеть должна обеспечить поддержку посредника;
- возможно возникновение задержек;
- посредник должен принимать участие в каждой транзакции, являясь узким местом в реализации протокола;
- при попытке взлома сети - посредник слабое звено, так как каждый участник протокола должен доверять ему.

2.1.2. Арбитражные протоколы

Арбитражный протокол делится на два подпротокола:

- протокол без посредника - он выполняется, если стороны смогли самостоятельно договориться;
- фактически протокол с посредником, которого приглашают в случае разногласия между сторонами (здесь посредника называют арбитром).

Арбитр - это незаинтересованное лицо, участвующее в протоколе. Арбитру доверяют обе стороны. Его приглашают для проверки честности выполнения протокола между сторонами. Хороший арбитражный протокол может не только определить факт мошенничества, но также и определить сторону, которой были совершены злодеяния. Такой протокол лишь обнаруживает мошенничество, но не предсказывает и не предотвращает его.

2.1.3. Самодостаточные протоколы

Такие протоколы считают лучшими, так как они обеспечивают полную честность сторон. Для такого протокола не требуется участие какого-либо посредника, даже в критические моменты. Протокол построен так, что при попытке одной стороны смошенничать - другая сразу узнает об этом, а протокол прекратит выполняться. Однако надо понмать, что не сущетсвует такого самодостаточного протокола, который подходил бы под все ситуации.

2.1.4. Попытки вскрытия протоколов

Существует много способов взломать протокол. Можно просто подслушивать протокол, пробуя добыть информацию - это **пассивное вскрытие**, здесь взломщик никак не воздействует на сам протокол. Такой тип взлома относится к взлому с использованием шифротекста. Его сложно обнаружить, поэтому протоколы реализованы таким образом, чтобы предотвратить вскрытие. Другой способ - **активное вскрытие** , по сути - просто изменение протокола. Например, можно попробовать подменить сообщение, повторное оправить старое или внести новое.

Пассивные взломщики занимаются сбором информации и криптоанализом сообщений. Активные взломщики стараются получить доступ к ресурсам или ухудшить работу системы. Взломщиком может оказаться, кто угодно - даже участник протокола. Он может обманывать, выполняя протокол или наоборот не следовать протоколу вовсе. Такой взломщик - мошенник. Пассивные мошенники выполняют правила протокола, но стараются получить больше информации, чем предусмотренно протоколом. Активные нарушают работу протокола.

2.2. Распространение ключей

Для того чтобы создать и настроить надежную сеть необходимо безопасно распределять ключ - так, чтобы два конечных пользователя могли одновременно получить секретный сессионный ключ шифрования.

Параметры, определяющие качество протокола распространения ключей:

- результатом работы протокола является секретный сессионный ключ;
- окончание протокола подразумевает под собой успешную взаимную аутентификацию абонентов;
- внешний пользователь не должен иметь возможность получить общий сессионный ключ с кем-то из внутренних пользователей;
- добавление и удаление участников из сети производится без уведомления всех участников сети.

Сети бывают с выделенным доверенным центром и без. Второй вариант плох тем, что с ростом количества участников сети, количество пар мастер-ключей растет с квадратичной скоростью.

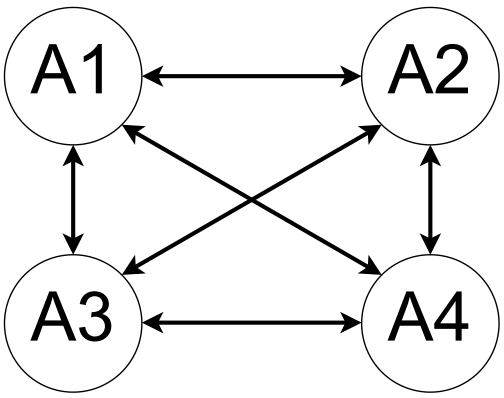

Рис. 1: Сеть без выделенного доверенного центра.

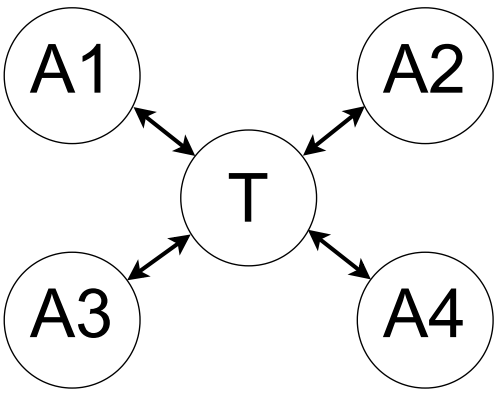

Рис. 2: Сеть с выделенным доверенным центром.

Протокол распространения ключей должен реализовывать следующие цели:

- аутентификация сторон протокола;
- защита от повтора;

- аутентификация ключа;
- подтверждение владения ключом;
- совершенная секретность;
- формирование новых ключей;
- ограниченная защита от атак и/или отказа в обсуживании.

Этап работы протокола с доверенным центром:

1) Доверенный центр создает секрет, известный только ему. Секрет из себя представляет пару из закрытого и открытого ключей.
2) Для каждого нового участника сети доверенный центр, используя секрет, создает сертификат, который позволяет новому участнику вырабатывать сеансовые ключи с другими участниками.
3) Здесь начинается общение участников. Они предъявляют друг другу идентификаторы, которые получили от доверенного центра. Далее используя эту информацию они могут сгенерировать секретный сеансовый ключ для общения мужду собой.

Изучим более подробно схемы распределения ключей с доверенным центром на примере протокола Жиро.

3. Протокол Girault

Протокол Жиро представляет из себя криптографический протокол, благодаря которому две стороны могут получить общий секретный ключ, не используя при этом явную сертификацию. Данный протокол использует полученный ключ для шифрования сообщений с помощью симметричного шифрования.

Схема Жиро решает проблему протоколов, основанных на подтверждении личности. Например, в схемах Шамира используются 2 атрибута - открытый ключ I и закрытый ключ s. Так как закрытый ключ s определяется непосредственно участником протокола, то он может начать выдавать себя за другого пользователя в любой момент. Также при возникновении противоречивых свидетельств у пользователя и подтверждающей стороны - невозможно определить, кто из них злоумышленник.

Жиро смог решить эту проблему, изменив процесс сертификации - ключи сами себя сертифицируют. В схеме Жиро присутствует доверенный центр, который позволяет пользователям обмениваться информацией по надёжному защищённому каналу. Теперь только доверенный центр может генерировать скрытую сертификацию для этих ключей. Надёжность схемы Жиро строится на стойкости криптосистемы RSA.
Первостепенно участники протокола проходят аутентификацию перед доверенный центром T, а также получают открытый ключ:

1) Начальный этап: доверенный центр T
   а) выбирает общий модуль $n = p \cdot q$, где p и q - большие простые числа;
   б) далее выбирает пару из закрытого $K_{T,priv} = (d, n)$ и открытого $K_{T,pub} = (e, n)$ ключей;
   в) выбирает элемент g поля $Z_n^{\times}$ максимального порядка;
   г) публикует в открытом доступе для участников параметры: n, e, g.
2) Основной этап: участники
   а) выбирают себе закрытый ключ s_i (каждый свой) и идентификатор I_i;
   б) вычисляют $v_i = g^{-s_i} mod n$;
   в) отправляют v_i доверенному центру;
   г) используя протокол аутентификации сторон участники доказывают доверенному центу T, что владеют закрытым ключом, не раскрывая его значение;
   д) далее получают от доверенного центра свой открытый ключ: $P_i = (v_i - I_i)^d = (g^{-s_i} - I_i)^d mod\ n$.
3) В результате для каждого участника будет выполняться: $P_i^e + I_i = g^{-s_i} mod\ n$.

Далее рассмотрим аутентификацию конечных участников. Пусть есть две стороны обычно их называют Alice и Bob, тогда процесс аутентификации между ними выглядит так:

1) Alice выбирает случайное R_A и передает Bob;

$$A \to \{I_A, P_A, t = g^{R_A}\ mod\ n\} \to B$$

2) Bob также выбирает случайное R_B;

$$B \to \{R_B\} \to A$$

3) Alice вычисляет значение y, которое смогла посчитать благодаря R_B;

$$A \to \{y = R_A + s_A \cdot R_B \ mod \ n\} \to B$$

4) Bob вычисляет $v_A = P_A^e + I_A \ mod \ n = g^{-s_A} \ mod \ n$;

5) Bob проверяет, что $t = g^y \cdot v_A^{R_B} = g^{R_A + s_a \cdot R_B} \cdot (g^{-s_A})^{R_B} = g^{R_A} \ mod \ n$;

Данные протокол построен на том, чтобы участник коммуникаций смог доказать, что он знает закрытый ключ, но при этом не сообщал значение этого ключа. При выполнении данного протокола вероятность того, что Bob примет сообщения Alice составляет практически 100% (стоит учитывать возможные помехи сети). В случае, если появится мошенник, который постарается выдать себя за участника протокола,то этот негодяй будет раскрыт с вероятностью $1 - 2^{-30}$.
А теперь рассмотрим поподробнее схему Жиро, в рамках которой генерируется общий секретный ключ и происходит обмен данными. По сути это, что происходит в пунктах 3 - 4 аутентификации.

3.1. Схема Жиро

Схема Жиро состоит из нескольких этапов обмена открытой информацией и вычисления ключа. Ниже опишем алгоритм протокола:

1) Alice посылает свой открытый ключ и идентификатор;

$$Alice \ \to \{P_A, I_A\} \to Bob$$

2) Bob вычисляет K:

$$K = (P_A^e + I_A)^{s_B} \ mod \ n$$

3) Bob высылает свои параметры:

$$Bob \ \to \{P_B, I_B\} \to Alice$$

4) Alice вычисляет K:

$$K = (P_B^e + I_B)^{s_A} \ mod \ n$$

.

В результате работы схемы стороны сгенерировали одинаковый общий сеансовый ключ.

$$K_{AB} = (P_A^e + I_A)^{s_B} = (g^{-s_A})^{s_B} = g^{-s_A s_B} \ mod \ n;$$

$$K_{BA} = (P_B^e + I_B)^{s_A} = (g^{-s_B})^{s_A} = g^{-s_A s_B} \ mod \ n;$$

$$K = K_{AB} = K_{BA} \ mod \ n;$$

Данная схема помимо генерации ключей обеспечивает также аутентификацию ключа - только легальные пользователи могут вычислить корректное значение общего сессионного ключа. А полученный ключ используется для шифрования дальнейшего обмена данными с помощью алгоритмов симметричного шифрования.

4. Криптографическая стойкость

Разберемся к каким атакам у данного протокола есть стойкость.

4.1. Защита от атаки подменой

Атака подменой - злоумышленник с помощью легально переданного сообщения составляет новое и передает его в следующем раунде протокола под видом другого сообщения.

Если ключи само сертифицированные, то нельзя проверить подлинность значений (I_A, P_A, s_A), так как они не подтверждены доверенным центром T.
Рассмотрим следующую ситуацию: появляется 3ий участник - Carol, который возьмет идентификатор Alice I_A и поддельный ключ s'_A, тогда он может вычислить значение $v_A = P_A^e + I_A = g^{-s_A} \ mod \ n$ и пройти аутентификацию перед T. Но вычислить s_A, зная v_A - это задачка дискретного логарифмирования, которая является неразрешимой. А без s_A Carol не сможет сформировать ключ K и соответственно продолжить притворяться Alice. Значит, протокол Жиро защищен от атаки подменой.

4.2. Защита от атаки повтором

Атака повтором - злоумышленник записывает все сообщения, проходящие в одном сеансе протокола, а далее повторяет их в новом, выдавая себя за одного из участников первого сеанса.

Пусть Carol перехватил сообщение Alice (I_A, v_A, s_A) и через некоторе время решает отправить его доверенному центру T. Проверив параметры, T поймет, что сообщение передано повторно, так как I_A уже использовался, и завершит сеанс. Таким образом, протокол Жиро защищен от атаки повтором.

5. Литература

Список литературы

[1] Брюс Шнайер - "Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке С."

[2] Венбо Мао - "Современная криптография. Теория и практика."

[3] Википедия - "Протокол Жиро."

[4] M. Girault - "Self-Certified Public Keys. C. 490—497."