Протокол

- Протоколом называют последовательность действий, исполняемых двумя или более сторонами, спроектированную для решения какой-либо задачи.

Характеристики

каждый участник должен протокол
каждый участник должен согласится следовать протоколу
протокол должен быть недвусмысленным
протокол должен быть полным - в нем должны быть указаны точные действия в любой возможной ситуации

Криптографический протокол

Дополнительное свойство

- Невозможно сделать или узнать больше,чем это определено протоколом

При разработке криптографического протокола мы должны ответить на следующие вопросы

Что есть модель атаки и реальна ли она?

Является ли протокол корректным?

Шнайер определяет криптографический протокол как протокол, в котором используется криптография. Вводится некоторый криптографический алгоритм

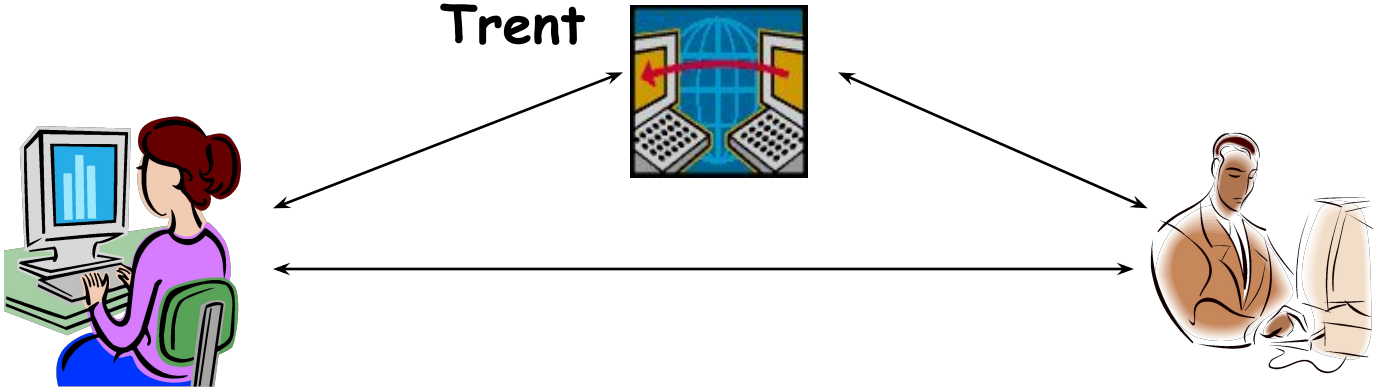
TEMPUS TACIS
CONTRACT #

Три типа протокола

- Протоколы с посредником:
  - Протокол требует участия незаинтересованной третьей стороны, которой доверено довести до конца исполнение протокола
    - Незаинтересованность означает, что ему безразличны как результат исполнения протокола, так и любой участник протокола
    - доверено – означает, что все участники протокола воспринимают его слова за истину.
- Протокол с арбитром
  - Третья сторона(снова незаинтересована и доверительна) вызывается только когда требуется определить честность выполнения протокла.
- Самодостаточные протоколы
  - Протокол разрабатывается для работы между двумя или более сторонами, не доверящим друг другу

TEMPUS TACIS
CONTRACT #

Протоколы с арбитром



Пример

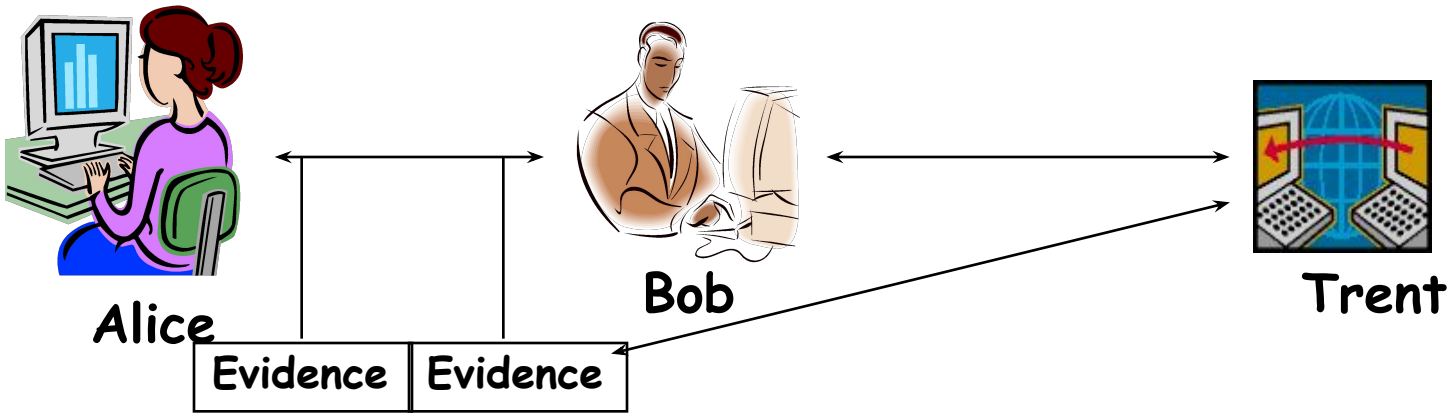
- Боб выписывает чек и передает его в банк
- Банк потдверждает чек, зарезервировав на счету Боба сумму денег, достаточную для погашения чека.
- Алиса передает право собственности Бобу, а Боб передает Алисе гарантированный чек
- Алиса депонирует чек

Проблемы

- Доверие - Будут ли доверять Алиса и Боб безликому арбитру затерянному в сети?
- Расходы – придется нести расходы, что может не понравится сторонам
- Задержка – При транзакции действия будут медленными
- Узкое место –Данную проблему может смягчить большее количество арбитров
- Уязвимость – так как арбитру должен доверять каждый пользователь сети, то он является лакомым кусочком для любого хакера

TEMPUS TACIS
CONTRACT #

Протокол с посредником



- Алиса и Боб соглашаются с условиями контракта
- Алиса подписывает контракт
- Боб подписывает контракт

Example

При разногласиях:

- Алиса и Боб предстают перед судом
- Алиса приводит свои доказательства
- Боб приводит свои доказательства
- Опираясь на доказательства, судья выносит приговор

TEMPUS TACIS
CONTRACT #

Самодостаточные протоколы

Alice

Bob

Свойства

- Арбитр не требуется
- Протокол честность
- Если одна из сторон пытается словчить, протокол прекращается

Это лучший тип протоколв

TEMPUS TACIS
CONTRACT #

Краткий экскурс

Основные понятия криптографии

Целью обсуждения протоколов является оценка неуязвимости протоколов при использовании определенных криптографических алгоритмов.

Мы рассмотрим системы в которых используется криптография и обсудим сложность разработки подобных систем

TEMPUS TACIS
CONTRACT #

Определения

Cryptography - Тайнопись

Plaintext - Исходное (читаемое) сообщение

Ciphertext - Зашифрованное сообщение

Encryption - преобразование исходного текста в зашифрованный текст

Decryption -восстановление исходного текста из зашифрованного

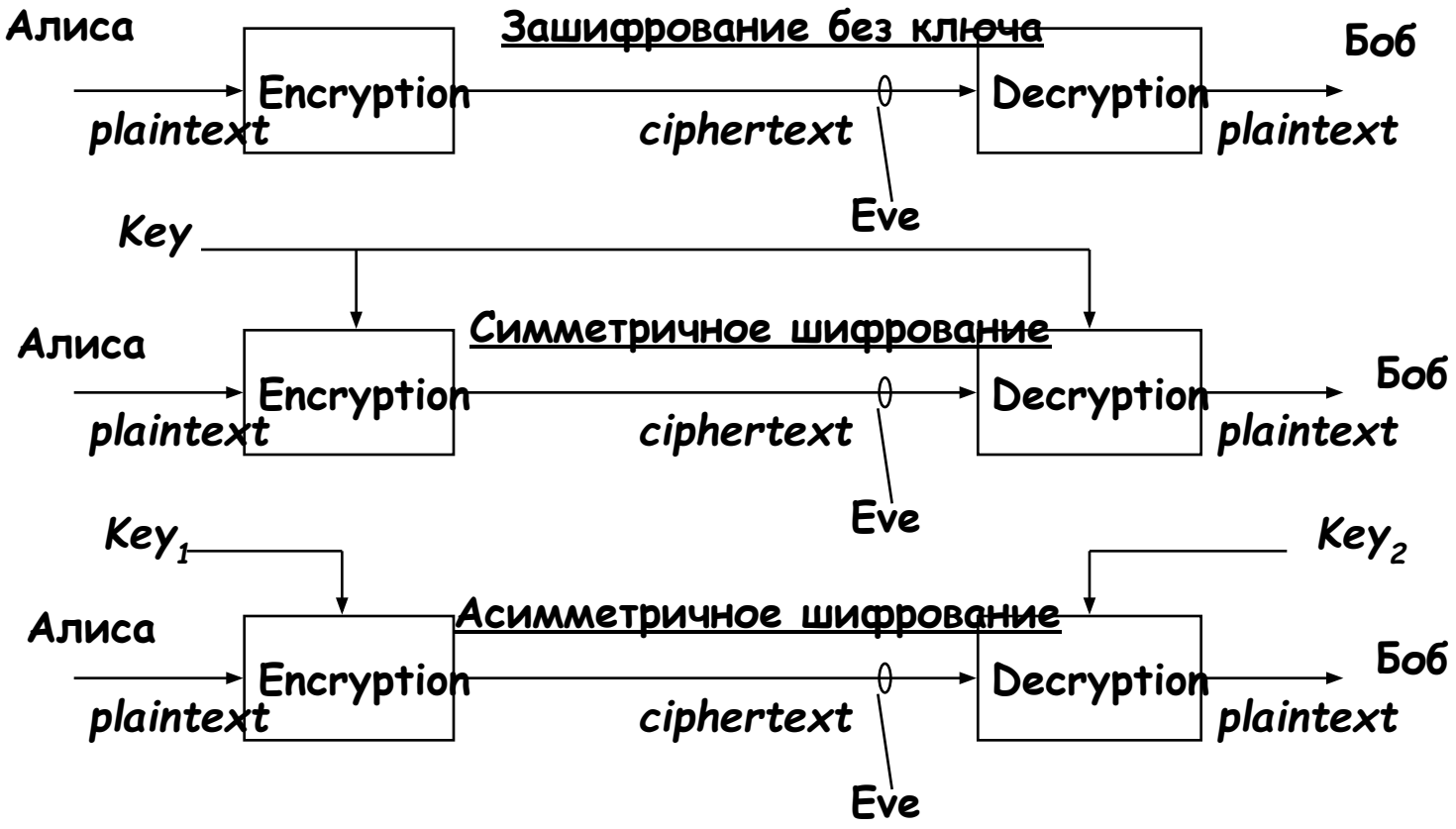
Key - дополнительная инф. используемая для зашифрования и/или расшифрования

Cryptanalysis - разработка способов вскрытия без знания ключа

Cryptology - криптография и криптоанализ

TEMPUS TACIS
CONTRACT #

Шифрование


Алиса
Зашифрование без ключа
Боб
Encryption
Decryption
plaintext
ciphertext
plaintext
Eve
Key
Алиса
Симметричное шифрование
Боб
Encryption
Decryption
plaintext
ciphertext
plaintext
Eve
Key1
Key2
Алиса
Асимметричное шифрование
Боб
Encryption
Decryption
plaintext
ciphertext
plaintext
Eve

Комментарий

Шифрование при отсутствии ключа:

Мы должны предположить, что Ева так же знает или может вскрыть алгоритм шифрования

Симметричное шифрование:

Поскольку Ева способна просматривать шифртексты, мы так же должны предположить, что она может просматривать каналы, по которым передается ключч

Асимметричное шифрование:

Один ключ полностью хранится в секрете, и второй доступен всем

Тайное голосование

Требования:

1) Участвовать в выборах могут только граждане, имеющие право голоса

2) Каждый избиратель может голосовать только один раз

3) Никто не может установить, за кого проголосовал каждый избиратель

4) Никто не может сделать дубликат бюллетеня с волеизъявлением любого избирателя

TEMPUS TACIS
CONTRACT #

Продолжение требований

5) Никто не может изменить результат голосования любого избирателя

6) Каждый избиратель может проверить,что его бюллетень учтен при подведении итогов голосования

Упрощенный протокол №1

1) Каждый избиратель шифрует свой бюллетень открытым ключом Центральной избирательной комиссии(ЦИК).

2) Каждый избиратель отсылает в ЦИК свой бюллетень

3) ЦИК расшифровывает бюллетени, подводит итоги и публикует результаты выборов

По многим причинам это абсолютно бесполезный протокол!

TEMPUS TACIS
CONTRACT #

Упрощенный протокол №2

1) Каждый избиратель подписывает бюллетень своим закрытым ключом.

2) Каждый избиратель шифрует свой бюллетень открытым ключом ЦИК.

3) Каждый избиратель отсылает свой бюллетень

4) ЦИК расшифровывает бюллетени, проверяет подлинность подписей, подводит итоги и публикует результаты выборов

Требования 1 и 2 удовлетворяются, но ЦИК знает кто как голосовал

Для решения этой проблемы нам необходимо использовать "Слепые подписи

Подписи вслепую

Данный тип цифровой подписи используется, когда необходимо подписать документ не видя его.

(По очевидным причинам метод используется не часто, так как никому не хотелось бы подписывать документ не зная что он содержит.)

Айгуль маскирует ее документ используя маскирующие множители.(Умножает сообщение на случайное число, которое называется маскирующий множитель)

Айгуль посылает "слепой" документ Болату

Болат подписывает документ вслепую и возвращает результат

Айгуль отделяет маскирующий множительи получает подписанный документ

Голосование через подписи вслепую

1) Каждый избиратель генерирует 10 наборов сообщений. В каждый набор включается достоверный бюллетень для каждого возможного итога голосования. Н-р За и Против. Для каждого сообщения генерируется случайный идентификационный номер, достаточно большой. Номер включается в бюллетень

2) Каждый избиратель маскирует все сообщения и посылает их в ЦИК

3) ЦИК проверяет по своей БД, что избиратель ранее не присылал на подписание свои маскированные бюллетени. Далее ЦИК открывает 9 наборов из 10 и проверяет на правильность оформления. ЦИК подписывает оставшийся бюллетень и отсылает избирателю, сохранив имя в БД.

TEMPUS TACIS
CONTRACT #

Продолжение протокола

4) Избиратель демаскирует сообщение и открывает набор бюллетеней, подписанной ЦИК

5) Каждый избиратель выбирает любой бюллетень и шифрует его открытым ключом ЦИК

6) Избиратель отсылает свой бюллетень

7) ЦИК расшифровывает бюллетень, проверяет на подлинность подписи, проверяет по БД уникальность ИД, сохраняет порядковый номер и включает его в итоги голосования. Затем ЦИК публикует результаты выборов вместе со всеми порядковыми номерами и соответствующим волеизъявлением.

TEMPUS TACIS
CONTRACT #

Анализ

ЦМК проверяет имеет ли права голоса данный избиратель

Метод голосования вслепую гарантирует, что ЦИК не может узнать кто как голосовал и у кого какой идентификационный номер

Идентификационные номера гарантирует, что никто не будет голосовать дважды

Каждый избиратель может проверить учтен ли его голос по спискам публикуемым ЦИК

Недостатки

Если этап 6 не анонимен и ЦИК может записать, кто какой бюллетень прислал, то ЦИК может и узнать, кто за что голосовал

Коррумпированная ЦИК может сгенерировать большое количество достоверных бюллетеней и отослать их самой себе.

Если избиратель обнаружит подмену своего бюллетеня, он не сможет этого доказать.

TEMPUS TACIS
CONTRACT #

Разделение функций

Решением проблемы может быть разделение функций между ЦИК и другой организацией

Пусть это будут ЦИК и ЦУР(Центральное управление регистрации)

Например, ЦУР определяет кто имеет право голосовать. ЦИК подсчитывает голоса.

TEMPUS TACIS
CONTRACT #

Выборы с двумя избирательными комиссиями

1) Каждый избиратель посылает в ЦУР письмо, запрашивая регистрационный номер.

2) ЦУР отправляет избирателю случайный регистрационный номер. ЦУР сохраняет список регистрационных номеров.

3) ЦУР Отсылает в ЦИК список регистрационных номеров.

4) Каждый избиратель выбирает случайный идентификационный номер. Он генерирует сообщение, состоящее из этого номера, регистрационного номера и своего бюллетеня.

5)ЦИК сверяет рег. Номер со списком полученным на этапе 3 от ЦУР. Если рег.номер в списке уже есть, ЦИК вычеркивает его. Затем ЦИК включает идент.номер в список номеров избирателей, проголосовавших за конкретного кандидата, и прибавляет единицу к его результату.

6) После получения всех бюллетеней ЦИК публикует результаты вместе со списками ИД и соответствующими бюллетенями.

TEMPUS TACIS
CONTRACT #

Анализ

Будем полагать, что все сообщения зашифрованы и подписаны.Это помешает кому-то выдавать себя за другого и перехватывать сообщения.

Несмотря на все меры, ЦУР должна быть доверенным органом власти, поскольку может регистрировать неправомочных избирателей, либо регистрировать правомочных несколько раз. Однако, если ЦУР публикует список зарегистрировавшихся избирателей(но без рег. номеров), то при числе зарегистрировавшихся избирателей меньшем чем число подсчитанных голосовать можно заподозрить махинации.

Протокол уязвим к сговору ЦИК и ЦУР

TEMPUS TACIS
CONTRACT #

Тайные многосторонние вычисления

Протокол **тайных многосторонних вычислений** позволяет группе людей вычислять любые функции нескольких переменных. Каждый участник предоставляет одну или несколько переменных. Результат становится известным всей группе, однако никто не знает входных значений других участников группы. На следующих слайдах мы рассмотрим несколько примеров

TEMPUS TACIS
CONTRACT #

Протокол 1

Средняя зарплата:

1. Алиса выбирает случайное число, и добавляет его к сумме своей зарплате. Она шифрует результат открытым ключом Боба и отсылает ему результат

2. Боб расшифровывает сообщение и добавляет сумму своей зарплаты. Затем шифрует его открытым ключом Кэрол и отсылает ей результат.

3. Кэрол делает то же самое и отсылает результат Дэйву зашифрованный его открытым ключом.

Протокол 1 продолжение

- Дэйв выполняет аналогичные действия, шифрует результат открытым ключом Алисы и отсылает ей.
- Алиса расшифровывает сообщение, вычитает свое случайное число и делит результат на количество на число людей в группе

Протокол 2

Алиса и Боб поспорили в ресторане о том, кто старше. Никто, разумеется. Не хочет сообщать другому свой возраст

Эту можно было бы разрешить с помощью третьего лица

Данную задачу еще называют проблемой миллионера Яо(Уао). См. Брюс Шнайер. Прикладная криптография. Стр. 613

Протокол 3

Алиса и Боб являются клиентами Службы тайных многосторонних знакомств.

Каждый из них имеет свое, скажем хобби, и хотел бы найти партнера, который имел бы точно такое же хоби. Но они не хотят раскрывать своих пристрастий.

Создаем внушительный список пристрастий. Теперь Алиса и Боб, разделенные модемной линией связи, могут участвовать в защищенном протоколе.

TEMPUS TACIS
CONTRACT #

Решение

- Алиса хэширует свой фетиш в семизначную строку.
- Она использует его как телефонный номер, звонит по этому номеру и оставляет сообщение для Боба.
- Если никто не отвечает она хэширует телефонный номер и повторяет эту операцию пока ей не помогут на том конце провода.
- Алиса сообщает Бобу сколько раз она применили операцию хеширования.
- Боб хеширует свой фетиш столько же раз сколько и Алиса. Он так же использует семизнаную строку результата как телефонный номер.

TEMPUS TACIS
CONTRACT #

Проблема обедающих криптографов

Три криптографа обедают в своем любимом трехзвездочном ресторане. Официант сообщает им, что метродатель принял необходимые меры для анонимной оплаты счета. За обед может заплатить один из криптографов или АНБ. Три криптографа признают право каждого заплатить анонимно, но им интересно, заплатит ли АНБ.

Дэвид Чаум

Применение этого протокола выходит далеко за рамки кружка за обеденным столом. Это пример безусловного неотслеживания отправителя и получателя.

TEMPUS TACIS
CONTRACT #

Метод

Пусть криптографами будут Алиса, Боб и Кэрол.

- Алиса бросает монетку и показывает результат Бобу (но не Кэрол).
- Боб бросает монетку и показывает результат Кэрол(но не Алисе).
- Кэрол бросает монетку и показывает результат только Алисе.
- Каждый криптограф объявляет как упали две монетки одинаково или нет. Если один из криптографов хочет оплатить счет, он утверждает обратное.
- Если число ответов "по-разному" будет нечетным, это означает, что обед оплачивает криптограф. Иначе АНБ

TEMPUS TACIS
CONTRACT #

Решение

Чтобы, понять как это работает, представьте, что Алиса пытается узнать, кто из двух других криптографов оплатил обед(при условии, что платила не она и не АНБ). Далее попытайтесь провести анализ самостоятельно.

- Пользователи располагаются по кругу
- Через регулярные интервалы времени соседние пары пользователей подбрасывают монетку, используя какой-нибудь протокол подбрасывания монетки "по телефону", защищенный от злоумышленников
- После каждого броска каждый пользователь заявляет "одинаково" или "по-разному".

TEMPUS TACIS
CONTRACT #

Обобщение

1. Этот протокол можетбыыть обобщен для любого количества криптографов

2. Это пример безусловного неотслеживания отправителя и получателя.

- Пользователи располагаются по кругу

- Через регулярные интервалы времени соседние пары пользователей подбрасывают монетку, используя какой-нибудь протокол подбрасывания монетки "по телефону", защищенный от злоумышленников

- После каждого броска каждый пользователь заявляет "одинаково" или "по-разному".

TEMPUS TACIS
CONTRACT #

Цифровые деньги

Цель:

Неотслеживаемость оплаты

Чеки и кредитные карточки имеют аудиторский след: вы не можете скрыть, кому платили деньги

Требования для цифровых денег:

Алиса может переслать деньги Бобу, так, чтобы Ева об этом не узнала.

Боб может оплатить счет Алисы в своем банке. Но банк не может идентифицировать Алису.

TEMPUS TACIS
CONTRACT #

Протокол 1

1. Алиса подготавливает 100 анонимных денежных переводов, каждый на сумму 1000$
2. Алиса высылает их в банк
3. Банк открывает 99 переводов и убеждается, что каждый перевод выписан на сумму $1000
4. Банк подписывает вслепую оставшийся перевод и списывает с ее счета $1000. Банк возвращает Алисе ее подписанный перевод
5. Алиса использует подписанный счет для оплаты покупки у торгавца
6. Торговец проверяет подпись банка
7. Торговец вручает денежный перевод банку
8. Банк проверяет подлинность своей подписи и перечисляет $1000 на счет торгавца

Протокол 2

Проблемой предыдущего протокола является возможность повторного использования Алисой перевода.

Пересмотр протокола

Алиса к каждому из своих 100 ден. Переводов прикладывает случайную строку

Когда банк оплачивает счет тогрговца, он сначала проверяет по своей БД, что перевод с данной уникальной строкой ранее не оплачивался. Иначе он отказывается принять его

TEMPUS TACIS
CONTRACT #

Протокол 3

Предыдущий протокол защищает банк от жуликов, но не позволяет установить их личности.

Торговец просит Алису вписать уникальную идентификационную строчку на денежном переводе.

Банк сравнивает идентифицирующую строку на денежном переводе с соответствующей строкой в базе данных. Если они совпадают, банк убеждается, что копия перевода сделана торговцем. Если идентифицирующие строки различаются, то чек копировала Алиса.

Требования

Требования к идеальной системе цифровых денег

1. Независимость. Надежность цифровых денег должна быть независима от местанахождения. Наличные могут передаваться по компьютерным сетям.

2. Защищенность. Цифровые деньги невозможно скопировать и использовать повторно.

3. Тайна частной жизни. (неотслеживаемость) Частная жизнь пользователя должна быть защищена.

TEMPUS TACIS
CONTRACT #

Требования продолжение

4. Оффлайновость платежей. При оплате пользователем покупки цифровыми деньгами, протокол между пользователем и продавцом должен исполнятся в оффлайновом режиме. Иными словами, для обработки платежа пользователя торговцу не обязательно соединяться с хостом.

5 Переносимость. Цифровые деньги должны допускать возможность передачи другим пользователям.

6. Делимость. Часть данной суммы цифровых денег можно разделить на меньшие суммы

TEMPUS TACIS
CONTRACT #