Протоколы и их классификация

Алгоритм — это конечная последовательность действий, направленная на решение некоторой задачи:

$$X \to A_1 \to A_2 \to A_3 \to \ldots \to A_n \to Y, \qquad (1)$$

X — исходные данные, Y — решение, A_j — элементарное j-тое действие.

Определение. Протокол (*protocol*) — описание последовательности алгоритмов, в процессе выполнения которой два или более участников последовательно исполняют эти алгоритмы и обмениваются сообщениями с целью решения некоторой поставленной перед ними задачи.

В качестве участников (субъектов, сторон) протокола могут выступать не только пользователи или абоненты, но и клиентские и серверные приложения.

Протоколы и их классификация

Пусть A_j^i — это элементарное j-тое действие выполняемое i-тым субъектом, X — исходные данные, необходимые для решения некоторой задачи, Y — её решение. Тогда конечная последовательность действий:

$$X \to A_1^1 \to A_2^1 \ldots \to A_{j_1}^1 \to A_1^2 \to \ldots \to A_{j_2}^2 \to A_1^{i_3} \to \ldots \to A_{j_3}^{i_3} \ \ldots$$

$$\ldots \to A_1^{i_n} \to \ldots \to A_{j_n}^{i_n} \to Y, \qquad (2)$$

направленная на получение Y, называется *протоколом*. При этом n — число *проходов* протокола. Для любого s $(3 \le s \le n)$ $i_s \in \{1, 2, \ldots, k\}$ является индексом участника протокола, где k — число участников протокола с обязательным условием $k \ge 2$. Наконец, $\sum_{t=1}^{n} j_t$ — число *шагов* протокола.

Протоколы и их классификация

Криптографическим протоколом (*cryptographic protocol*) называется любой протокол, в котором используются криптографические системы и криптографические алгоритмы.

Шаг протокола (*step of protocol*, *protocol action*) — это элементарное законченное действие в протоколе с точки зрения его описания. Например, шагами могут быть: вычисление значения функции, генерация случайного числа, сравнение двух чисел, отправка сообщения.

Проход (*цикл* или *раунд*) протокола (*pass of cryptographic protocol*, *round*,) — это максимальная последовательность шагов протокола, непрерывно выполняемая одной из сторон. Проход заканчивается передачей активности другому участнику протокола, что, как правило, выражается формированием и отправкой сообщения другой стороне.

Протоколы и их классификация

Сеанс (*session*) — это конкретная реализация протокола с конкретными участниками.

Роль – это функция, которую выполняет одна из сторон протокола в процессе выполнения сеанса. Таким образом, ролей не больше числа участников протокола, поскольку одну и ту же роль могут выполнять несколько участников. Например, всегда у кого-то есть роль *инициатора*, а у кого-то роль *ответчика*.

Роли и действующие лица криптографических протоколов естественно возникли в ходе их описания. В дальнейшем для облегчения описания и восприятия работы протоколов за участвующими сторонами протоколов закрепили определенные имена сначала в порядке латинского алфавита, далее по ролевым характеристикам.

Протоколы и их классификация

1) Основные действующие лица:
   - A: Алиса (Alice) — как правило исполняет роль инициатора протокола;
   - B: Боб (Bob) — отвечает на инициативу Алисы.
2) Если протокол требует участия третьей или четвертой стороны, в игру вступают:
   - C: Кэрол (Carol) — участница в трёх- или четырёхсторонних протоколах в качестве третьей стороны;
   - D: Дэйв (Dave) — участник четырехсторонних протоколов в качестве четвертой стороны.

Протоколы и их классификация

3) Остальные участники играют специальные вспомогательные роли (претендентов, противников и контролеров) и появляются по мере надобности:
   - E: Ева (Eve) — перехватчица сообщений (пассивная);
   - M: Мэллори (Mallory) — злонамеренная активная взломщица;
   - T: Трент (Trent) — доверенный посредник;
   - W: Уолтер (Walter) — надзиратель, в некоторых протоколах стережёт Алису и Боба;
   - P: Пегги (Peggy) — претендентка, пытается доказать что-то;
   - V: Виктор (Victor) — верификатор, проверяет Пегги.

Протоколы и их классификация

Основными характеристиками криптографического протокола являются:

- *Прозрачность*. Каждый участник протокола должен знать протокол и всю последовательность его действий.
- *Однозначность*. Действие каждого участника в протоколе должно быть однозначно определено.
- *Полнота*. Протокол должен быть полным — в нем должны быть указаны точные действия в любой возможной ситуации.

Протоколы и их классификация

Основные задачи криптографических протоколов:

- ✓ Конфиденциальность (секретность какой-либо части информации);
- ✓ Аутентичность (подтверждение целостности или авторства);
- ✓ Неотслеживаемость предметов и субъектов протокола.

Основное требование к криптографическому протоколу гласит, *чтобы невозможно было сделать или узнать больше, чем определено протоколом*.

Протоколы и их классификация

Простейшим протоколом является ПРОТОКОЛ СЕКРЕТНОЙ СВЯЗИ, описываемый следующими шагами:

Шаг 1. Алиса шифрует сообщение M с помощью своего ключа E, получает криптограмму $Y = E(M)$.

Шаг 2. Алиса отправляет криптограмму Y Бобу.

Шаг 3. Боб принимает сообщение Y.

Шаг 4. Боб расшифровывается полученное сообщение с помощью своего ключа D, получает открытое сообщение $M = D(Y)$.

Протоколы и их классификация

Это однопроходный протокол, схематическая запись которого имеет следующий вид.

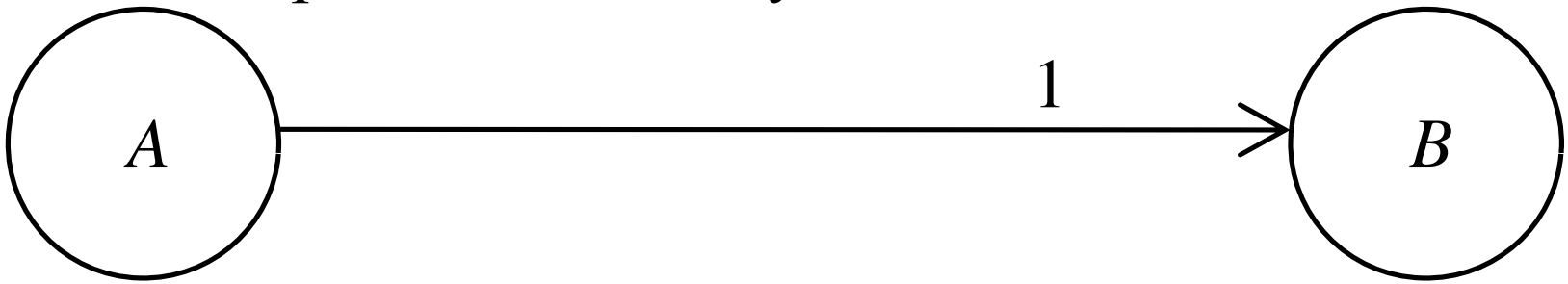


Рис. 1

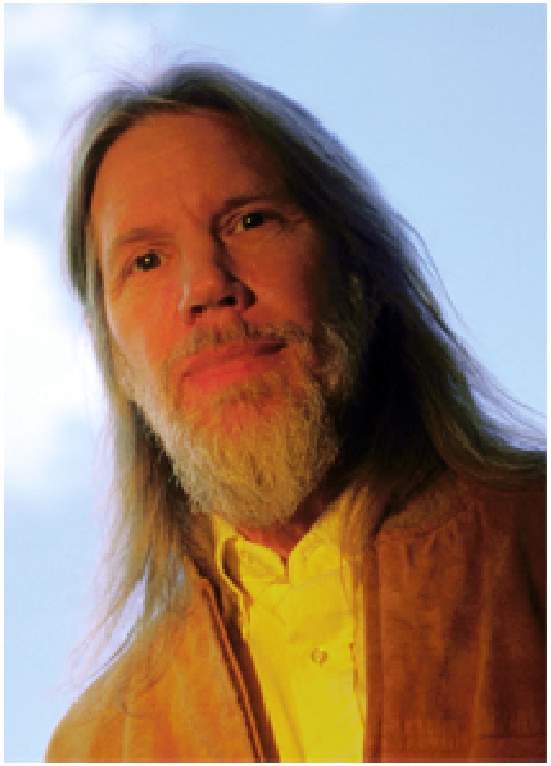
1. $A \rightarrow B$: $Y = E(M)$, (Алиса вычисляет криптограмму $E(M)$ и отправляет её Бобу).
2. B: $M = D(Y)$, (Боб принимает и расшифровывает криптограмму Y Алисы).

Протоколы и их классификация

В дальнейшем будем использовать краткую схематическую запись протоколов, если она не нарушает однозначного прочтения всех шагов протокола. Краткая схематическая запись, как правило, ограничивается указанием содержания проходов протокола.

В простейшей форме протокола (Рис. 1) очень трудно заметить, что сама последовательность шагов, может решить совершенно новую задачу, лежащую за пределами используемых алгоритмов в шагах протокола. Поэтому появление собственной теории криптографических протоколов связывают с появлением протокола распределения ключей Диффи и Хеллмана (Whitfield Diffie, Martin Hellman) в 1976 году.

Протоколы и их классификация



Бе́йли Уи́тфилд Ди́фф и (англ. *Bailey Whitfield 'Whit' Diffie*; родился 5 июня 1944, Куинс, Нью-Йорк, США) — один из самых известных американских криптографов, заслуживший мировую известность за концепцию криптографии с открытым ключом.

Ма́ртин Э́двард Хе́ллма н (англ. *Martin Edward Hellman*; род. 2 октября 1945, штат Нью-Йорк) — американский криптограф. Получил известность благодаря разработке первой асимметричной криптосистемы в соавторстве с Уитфилдом Диффи и Ральфом Мерклем (1976). Один из активных сторонников либерализации в сфере криптографии.

Протоколы и их классификация

Классификация по степени развития

1) Минимальные протоколы, т.е. такие протоколы, в которых уже не удается выделить никакого собственного подпротокола, называют *элементарными* или *основными*, или *примитивными*. Их также называют *криптографическими примитивами*.
2) Иногда в протоколе удается выделить подпротокол, т.е. такую непрерывную подпоследовательность действий, которая решает некоторую промежуточную задачу, не являющуюся конечной задачей никакого прикладного протокола. Такие протоколы называются *промежуточными*.
3) Протоколы, состоящие из нескольких примитивных или промежуточных, называют *развитыми*. Также их часто называют просто *прикладными протоколами*, поскольку они решают практические задачи обеспечения безопасности и, как правило, сразу же по нескольким функциям.

Протоколы и их классификация

Классификация по степени участия незаинтересованных сторон

1) *Протоколы с посредником*, т.е. такие протоколы, в которых прописано обязательное участие третьей незаинтересованной стороны (адвокатов, нотариусов, независимого центра распределения, центрального сервера и т.п.). Ясно, что эта сторона должна иметь высокий уровень надёжности и доверия. В первую очередь именно на этом факте держится устойчивость таких протоколов.
2) *Протоколы с арбитром*, т.е. такие протоколы, в которых третья незаинтересованная сторона вступает в действие только в некоторых сценариях исполнения протокола для полного его завершения. Как правила это связано с возникновением какого-либо конфликта в момент исполнения протокола.
3) *Самодостаточные протоколы*, т.е. такие протоколы, в которых третья незаинтересованная сторона отсутствует, и при этом протокол всегда проводится до конца по одному из своих сценариев.

Протоколы и их классификация

Классификация по числу проходов

1) *Неинтерактивные*, т.е. такие протоколы, в которых осуществляется только одна передача данных.
2) *Интерактивные*, т.е. такие протоколы, в которых осуществляется несколько передач данных. Среди них также иногда выделяют: *двухпроходные*, *трехпроходные* и т.д.

Классификация по числу участников

1) *Двухсторонние*.
2) *Трёхсторонние*, и т.д.
3) *Многосторонние*.

Классификация по типу используемой системы шифрования

1) *На основе симметричных криптосистем*.
2) *На основе асимметричных криптосистем*.
3) *Смешанные*.

Протоколы и их классификация

Классификация по типу решаемой задачи

1) *Протоколы распределения ключей.*
2) *Протоколы (схемы) цифровой подписи.*
3) *Протоколы (схемы) аутентификации.*
4) *Протоколы (схемы) разделения секрета.*
5) *Протоколы конфиденциальной передачи.*
6) *Игровые протоколы: протоколы подбрасывания монеты по телефону, протоколы игры в покер,* и т.п.
7) *Протоколы электронного голосования.*
8) *Протоколы оборота электронных денег.*

И т.д.

Протоколы и их классификация

Осталось заметить, что некоторые протоколы, которые решают особенно удивительные задачи, которые на первый взгляд противоречивы в своей постановке, иногда называют *изотерическими*. К ним в частности относят протоколы безопасных выборов, протоколы безопасных вычислений с несколькими участниками, протоколы анонимной широковещательной передачи сообщений, протоколы электронных наличных.