Федеральное государственное автономное образовательное учреждение высшего образования
Национальный исследовательский ядерный университет «МИФИ»

Кафедра «Криптология и кибербезопасность»

Криптографические протоколы

курс лекций

Запечников Сергей Владимирович,
профессор кафедры «Криптология
и кибербезопасность» НИЯУ МИФИ

Москва – 2018

Криптографические протоколы

Теоретическая часть (проф. Запечников С.В.)

8 занятий * 4 часа = 32 часа (08.02.2018 – 29.03.2018, кроме 08.03.2018)
Минимум для зачёта – 24 балла, максимум – 40 баллов

Посещение – 1 балл за каждые 2 часа занятий: минимума нет, максимум – 14 баллов
Большое домашнее задание (2-7 недели): минимум – 12 баллов, максимум – 26 баллов
Контрольная работа (8 неделя): минимума нет, максимум – 14 баллов

Лабораторный практикум (преп. Горлатых А.В.)

8 занятий * 2 часа = 16 часов (с 07.04.2018)
Минимум для зачёта – 36 баллов, максимум – 60 баллов

Лаб.работа № 1 – WireShark (минимум – 5 баллов, максимум – 8 баллов)
Лаб.работа № 2 – Аутентификация PAP, CHAP, S/KEY (минимум – 5 баллов, максимум – 8 баллов)
Лаб.работа № 3 – Протоколы транспортировки ключей (минимум – 5 баллов, максимум – 8 баллов)
Лаб.работа № 4 – Протоколы обмена ключей (минимум – 5 баллов, максимум – 8 баллов)
Лаб.работа № 5 – Гибридное шифрование (минимум – 8 баллов, максимум – 14 баллов)
Лаб.работа № 6 – Мини-исследовательский проект «APT-атаки» (минимум – 8 баллов, максимум – 14 баллов)

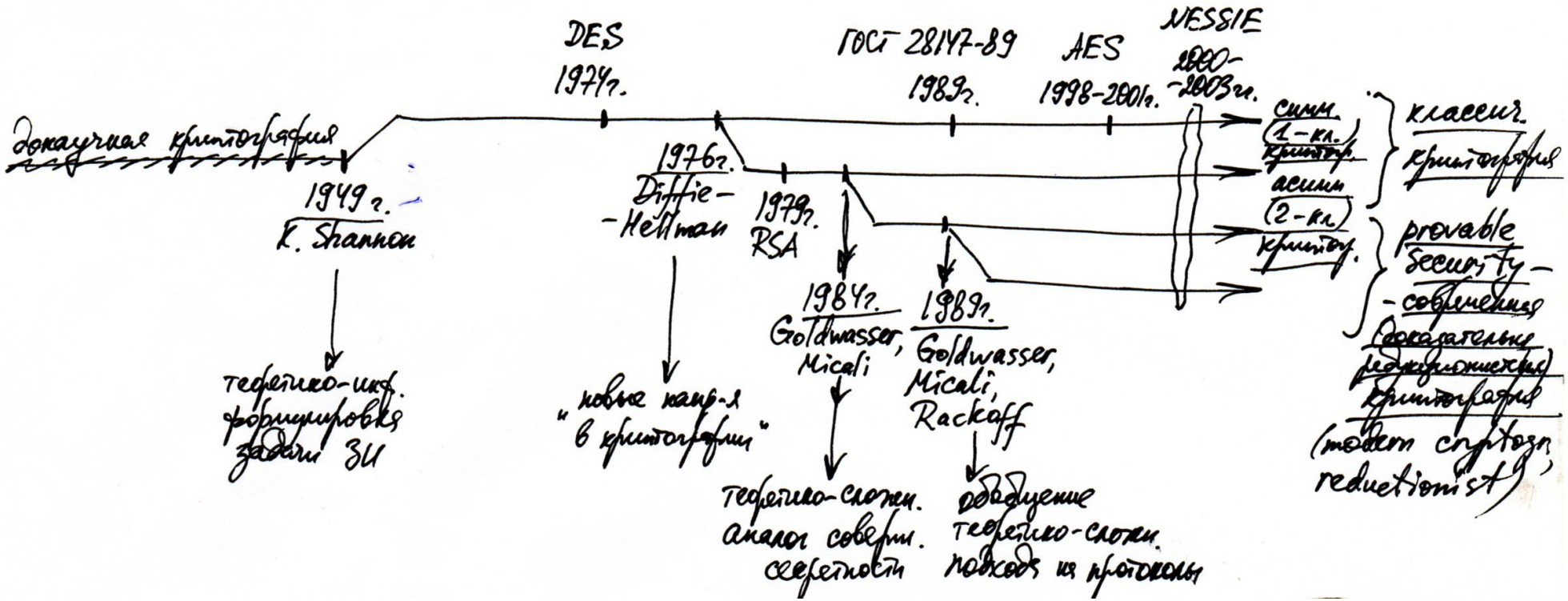
Криптографические протоколы

курс лекций

Лекция 1.
Введение. Основы конструирования и анализа криптографических протоколов

08 февраля 2018 г.

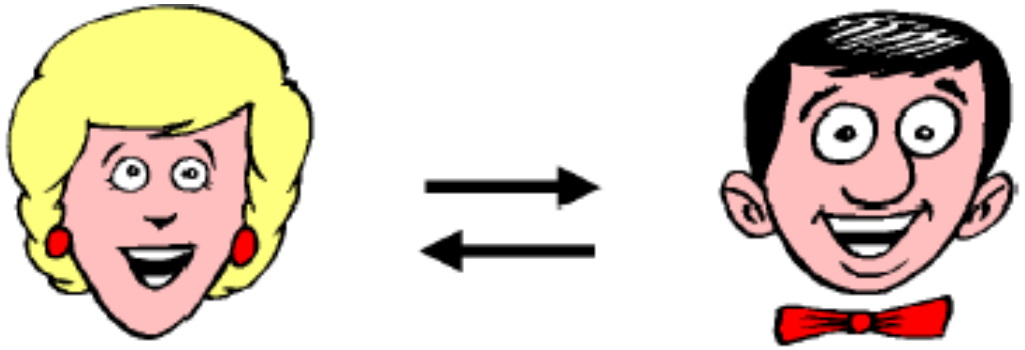
Исторические этапы развития криптографии




Системы защиты информации
Некриптографические системы и сервисы защиты
Криптографические системы (сервисы защиты)
Система защищенного электронного документооборота
Система электронных платежей
Система защищенного резервного копирования
Система электронного голосования
Сервис обеспечения стойкости к компрометации части ключей
… … …
… … …
Криптографические схемы (механизмы защиты)
Симметричные схемы шифрования
Схемы открытого шифрования
Симметричные схемы аутентификации сообщений
Схемы цифровой подписи
Схемы разделения секрета
… … … … … …
Криптографические протоколы
Двусторонние:
протокол «передачи со стиранием»;
протокол «депонирования бита»;
протокол «бросания монеты по телефону»;
протокол распределения ключей;
протокол аутентификации с нулевым разглашением знания;
и др.
Многосторонние:
протокол пороговой подписи;
протокол групповой подписи;
протокол разделения секрета;
протокол «византийского соглашения»;
и др.
Криптографические алгоритмы
бесключевые
одноключевые
двухключевые
«Строительные блоки» криптографических протоколов
вероятностные доказательства
способы распространения ключей
модели ключевых систем (в том числе PKI)
методы аутентификации субъектов компьютерных систем
и др.
Криптографические примитивы
Перемешивающие, инженерные (confusion/diffusion)
Алгебраические и комбинаторные
Базовые математические факты
теория информации
алгебра
теория чисел
комбинаторика
теория сложности вычислений
теория вероятностей
теория булевых функций
…
и др.

Основные понятия и определения (1)

- **Протокол – это последовательность шагов, точно специфицирующих действия, которые требуются от двух или более участников для решения некоторой задачи.**
- **Протокол – распределённый алгоритм!**



Свойства протокола:

1) действия имеют очерёдность от начала и до конца; ни одно действие не выполняется, пока не закончилось предыдущее;

2) должно быть точно определено каждое действие; не должно быть двусмысленности, из каждой ситуации должен быть определённый выход;

3) одного действующего лица недостаточно для протокола (должно быть 2 или более):

A, B (C, D, E, …);

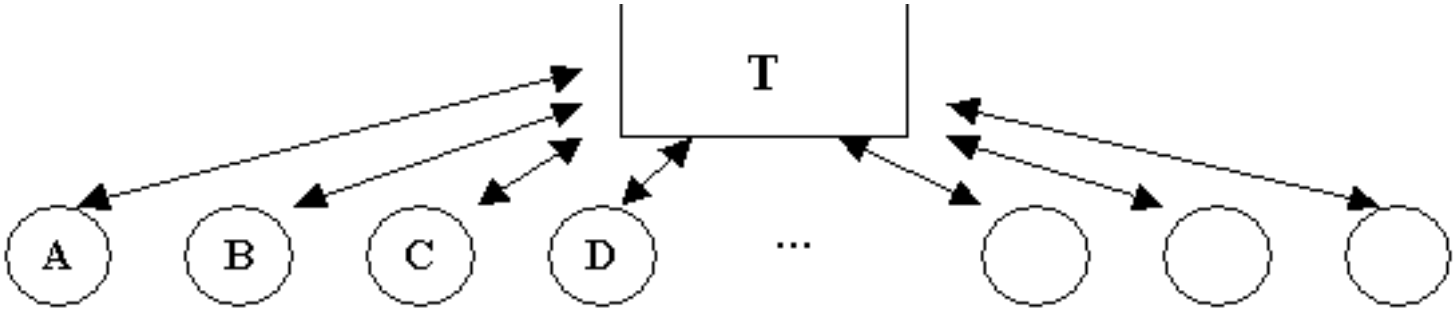
4) все участвующие в протоколе стороны должны заранее знать последовательность действий и быть согласны следовать этой последовательности;

5) стороны решают некоторую конкретную задачу.

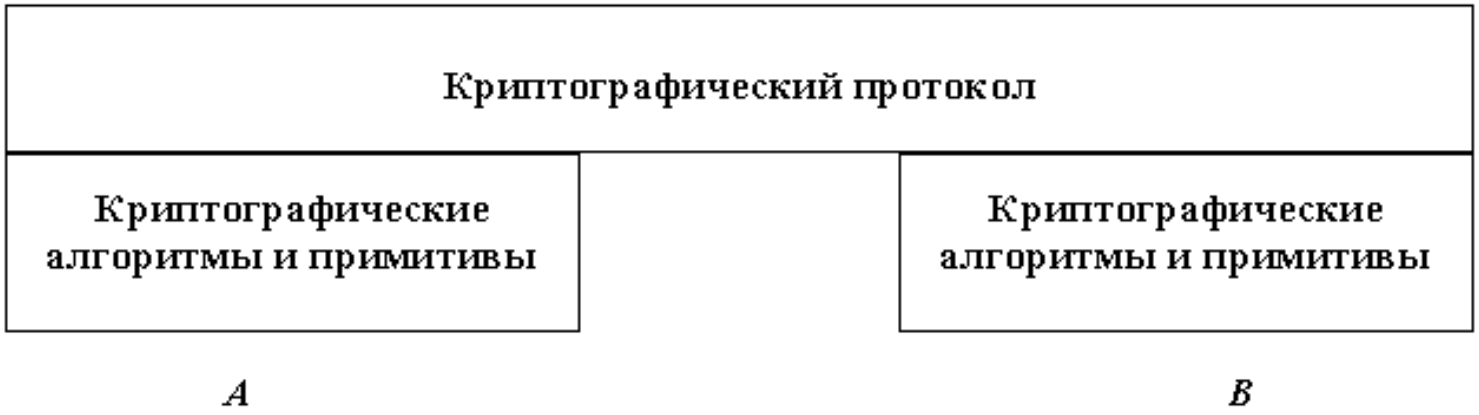
Основные понятия и определения (2)

- **Криптографический протокол — протокол, в котором используются криптографические алгоритмы и который служит для решения некоторой криптографической задачи.**

«Теоретическое» решение:



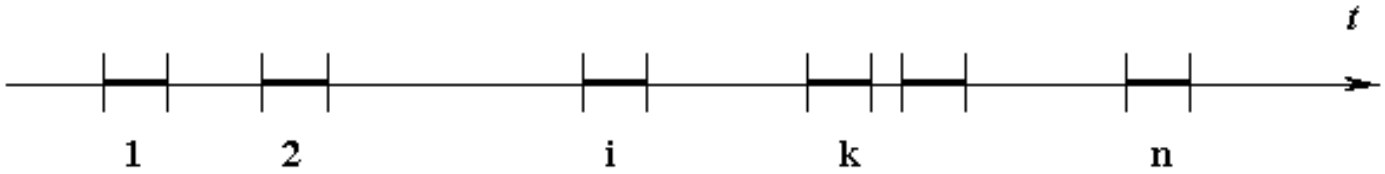
Реальное решение:



Основные понятия и определения (3)

Один и тот же протокол может выполняться одними и теми же лицами многократно в течение какого-то промежутка времени.

Сеанс (сессия) – это однократное выполнение протокола.



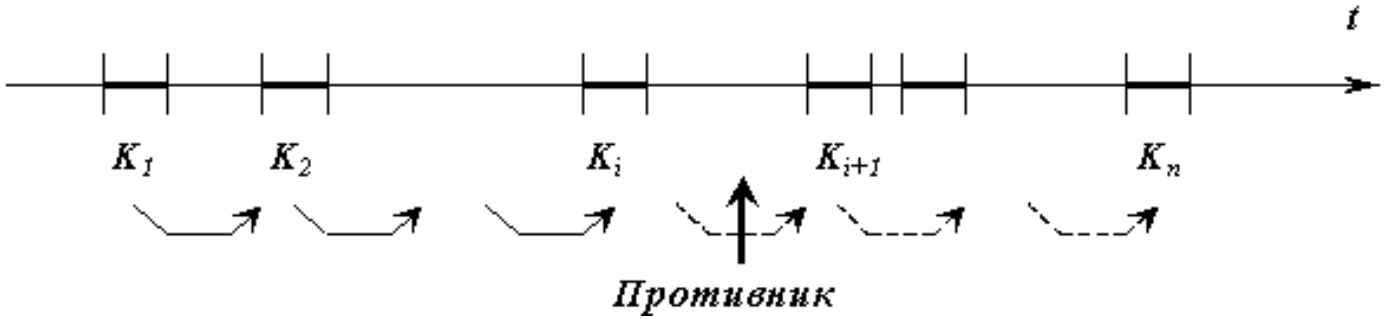
Участники протокола:

- ✓ **Основные и вспомогательные (центр доверия, удостоверяющий центр, центр распределения ключей и пр.).**
- ✓ **Честные и нечестные:**
  - активный противник;
  - пассивный противник.

Атаки на криптографические протоколы (1)

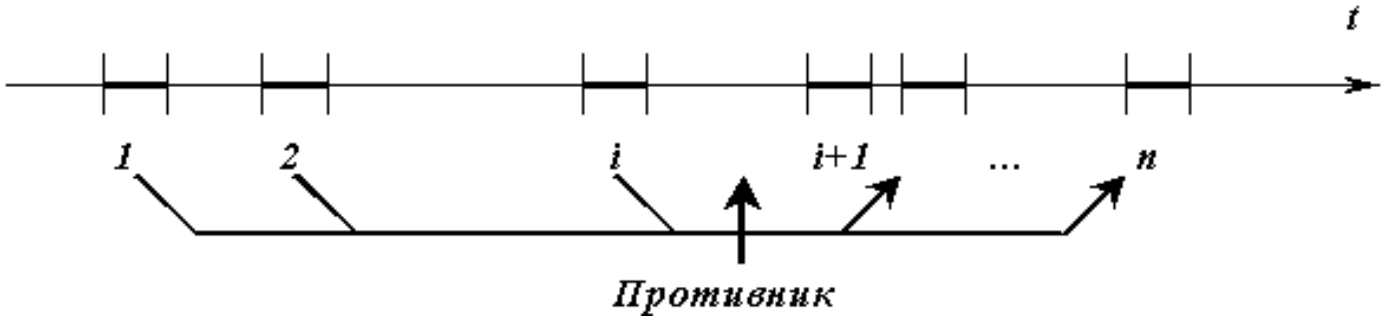
1. Атака по известным ключам.

Противник обладает некоторыми ключами, использованными в предыдущих сеансах протокола, и затем использует эту информацию для определения новых ключей в последующих сеансах (например, выявляет закон изменения ключей).



2. Атака методом повтора сеанса.

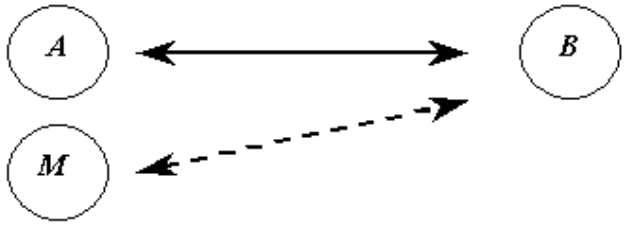
Противник полностью или фрагментарно записывает сеанс протокола и повторно применяет эти сообщения или их часть в одном из следующих сеансов.



Атаки на криптографические протоколы (2)

3. Деперсонификация («маскарад»).

Противник принимает на себя идентичность одного из законных (легальных) участников протокола.



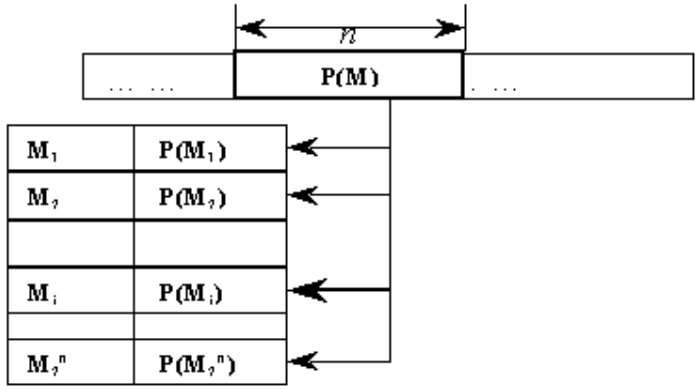
4. Словарная атака.

Атака путём перебора наиболее вероятных значений каких-либо величин или сообщений, передаваемых в протоколе (например, путём перебора паролей, в качестве которых довольно часто берутся фамилия, имя, отчество, номер телефона, адрес и т.п.).

Атаки на криптографические протоколы (3)

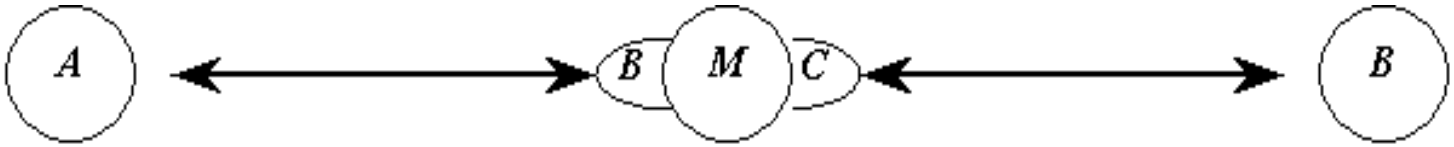
5. Атака методом опережающего поиска.

Атака по принципу осуществления похожа на словарную, но реализуется путём полного перебора всех возможных значений какой-либо величины, и используется, как правило, для расшифрования сообщений.



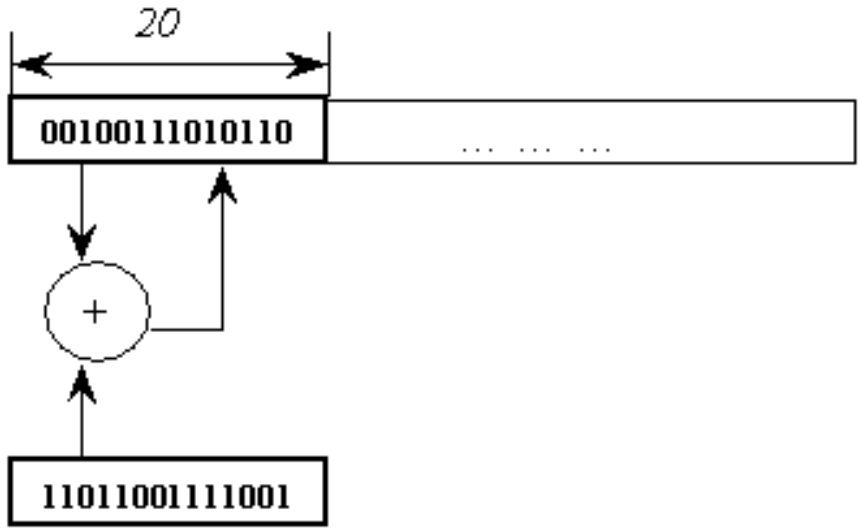
6. Атака методом включения в канал.

Противник *M* «врезается» в канал связи между законными участниками *A* и *B*, «пропускает через себя» все проходящие сообщения и искажая протокол между ними: может модифицировать, задерживать сообщения, менять их местами и т.п.



Компрометация криптографического протокола

Компрометация протокола – это ситуация, когда протокол не способен достичь тех целей, для которых он был предназначен, причём противник получает преимущество без непосредственного «вскрытия» нижележащих примитивов или алгоритмов, а только путём манипуляции протоколом.



Вероятностные доказательства

Интерактивные системы доказательства (1)

Интерактивная система доказательства *(interactive proof system)* **– протокол, включающий двух участников: *доказывающего* (*prover* – *P*) и *проверяющего* (*verifier* – *V*). Предварительно формулируется некоторое утверждение *S*, например, утверждение о том, что некоторый объект *w* обладает свойством *L*:** $w \in L$**. В ходе протокола *P* и *V* обмениваются сообщениями. Каждый из них может генерировать случайные числа и использовать их в своих вычислениях. В конце протокола *V* должен вынести свое окончательное решение о том, является ли *S* истинным или ложным.**

Цель участника *P* всегда заключается в том, чтобы убедить участника *V* в том, что *S* истинно, независимо от того, истинно ли оно на самом деле или нет. Таким образом, *P* может мошенничать в протоколе, так как *S* может быть ложно, т.е. он может быть активным противником. *V* должен проверять аргументы участника *P*. Цель участника *V* заключается в том, чтобы вынести решение, является ли *S* истинным или же ложным, то есть интересы участников протокола *P* и *V* не совпадают.

Интерактивные системы доказательства (2)

Однако участник *V* имеет полиномиально ограниченные вычислительные возможности, а именно время его работы ограничено некоторым полиномом от длины доказываемого утверждения: $t \le p(|w|)$. Это предположение является стандартным для моделирования вычислительных возможностей обычных средств вычислительной техники. В силу этого он самостоятельно, без помощи *P*, не способен распознать истинность утверждения *S*.

Вычислительные возможности *P* никак не ограничиваются, что в действительности может соответствовать ситуации, когда *P* владеет какой-то трудно получаемой информацией (хотя он может и обманывать, утверждая, что такая информация у него имеется).

Программа действий участника *V* должна быть устроена таким образом, чтобы:

1) если *S* истинно, *P* смог бы убедить *V* признать это;

2) если *S* ложно, *P* не смог бы убедить *V* в противном, какие бы аргументы он ни выдвигал, т.е. вне зависимости от получаемых от *P* сообщений.

***V* может ошибаться, но ставится условие, чтобы вероятность принятия им неправильного решения была бы пренебрежимо мала.**

Пример интерактивной системы доказательства, основанной на задаче теории чисел (1)

Зададимся натуральным числом *n*. Рассмотрим мультипликативную группу $Z_n^* = \{x < n; (x,n) = 1\}$**. Обозначим** $QR = \left\{(x,n) \middle| x < n, (x,n) = 1, \exists y : y^2 \equiv x \bmod n\right\}$ **– множество квадратичных вычетов числа *n*. Напомним, что если сравнение** $y^2 \equiv x \pmod n$ **имеет решение, то *x* называется квадратичным вычетом числа *n*. В противном случае *x* называется квадратичным невычетом. Тогда** $L = QNR = \left\{(x,n) \middle| x < n, (x,n) = 1, \nexists y : y^2 \equiv x \bmod n\right\}$ **– множество квадратичных невычетов числа *n*. *P* доказывает *V* утверждение** $S : (x,n) \in QNR$**.**

Задача распознавания квадратичных вычетов не решаема за полиномиальное время. В силу этого проверяющий, полиномиально ограниченный в своих вычислительных ресурсах, не может самостоятельно проверить истинность сформулированного утверждения.

Пример интерактивной системы доказательства, основанной на задаче теории чисел (2)

	P		*V*
1		$\leftarrow$	Для $i=\overline{1,k}, k=\lvert n \rvert$ выбирает: $b_i \in \{0,1\}$ – случайный бит, $z_i \in Z_n^*$ и вычисляет $(w_1,\ldots,w_k)$, где $w_i = \begin{cases} z_i^2 \pmod n, если (b_i = 1) \\ x \cdot z_i^2 \pmod n, если (b_i = 0) \end{cases}$
2	Для $i=\overline{1,k}$ вычисляет $(c_1,\ldots,c_k)$, где $c_i = \begin{cases} 1, если (w_i, n) \in QR \\ 0, если (w_i, n) \notin QR \end{cases}$	$\rightarrow$	
3			Принимает доказательство тогда и только тогда, когда для $\forall (i=\overline{1,k})$ $c_i=b_i$.

Свойства интерактивной системы доказательства (1)

Утверждение 1. **Для** $\forall x \in QNR$ **если** $(x,n) \in QNR$ **, т.е.** $\nexists y : y^2 \equiv x \pmod{n}$ **, то** ***P*** **докажет** ***V*** **утверждение** ***S*** **с вероятностью, равной 1.**

Доказательство: **Рассмотрим действия участника** ***V*** **на шаге (1) протокола.**

Когда b_i**=1, по условию протокола** $\exists z_i : z_i^2 \equiv w_i \pmod{n}$**. По определению вычета это означает, что** $(w_i, n) \in QR$**, т.е.** w_i **является квадратичным вычетом числа** ***n*****.**

Когда b_i**=0, по условию протокола** $z_i^2 \cdot x \equiv w_i \pmod{n}$ **. Из доказываемого утверждения известно, что** $(x,n) \in QNR$**. Может ли** w_i **быть квадратичным вычетом числа** ***n*****? Для этого должно быть:** $\left(z_i \cdot x^{\frac{1}{2}} \right)^2 \equiv w_i \pmod{n}$**. Это может быть, только если** ***x*****=1. Но** $(1,n) = 1$**. Кроме того,** $\exists y = 1 : y^2 \equiv 1 \pmod{n}$**. Следовательно,** $(1,n) \in QR$ **– мы пришли к противоречию с исходным утверждением.**

Следовательно, b_i**=0 тогда и только тогда, когда** $(w_i, n) \in QNR$**, т.е. мы установили однозначную связь:** w_i **является квадратичным вычетом числа** ***n*** **только при** b_i**=1. Распознавая** ***QR*** **на шаге (2) протокола (эту задачу нельзя решить за полиномиальное время), доказывающий** ***P*** **будет отвечать битом** c_i**=1 тогда и только тогда, когда** b_i**=1, т.е. на шаге (3) результат проверки всегда будет положительным, и** ***V*** **всегда примет доказательство.**

Свойства интерактивной системы доказательства (2)

Утверждение 2. **Для** $\forall x$ **если** $(x,n)\notin QNR$**, то вероятность ошибки** ***V*** **составляет** $\mathrm{P}_V^{ош}=\frac{1}{2^k}$.

Доказательство:

Когда b_i**=1, по условию протокола** $\exists z_i : z_i^2 \equiv w_i \pmod n$**. По определению вычета это означает, что** $(w_i,n)\in QR$**, т.е.** w_i **является квадратичным вычетом числа** ***n*****.**

Когда b_i**=0, по условию протокола** $w_i \equiv x\cdot z_i^2 \pmod n$**. Если** $(x,n)\notin QNR$**, т.е.** $(x,n)\in QR$**, то** $(x,n)=1, \exists y : y^2 \equiv x \pmod n$**. Тогда можно записать, что** $w_i \equiv y^2\cdot z_i^2 \pmod n$**, или, что то же самое,** $w_i \equiv (y\cdot z_i)^2 \pmod n$**. Значит,** $\exists v = y\cdot z_i : v^2 \equiv w_i \pmod n$**, т.е.** $(w_i,n)\in QR$**. Итак,** w_i**– случайный квадратичный вычет числа** ***n*****.**

В любом случае: b_i**=0 или** b_i**=1 – участник** ***P*** **на шаге (2) протокола всегда будет распознавать число** w_i **как квадратичный вычет числа** ***n*****. Следовательно, он может угадать, какой бит** $b_i=\{0,1\}$ **был выбран, только случайно, с вероятностью** $\mathrm{P}=\frac{1}{2}$**. Следовательно, все** ***k*** **бит** $\{b_1,\ldots,b_k\}$ **он сможет угадать лишь с вероятностью** $\mathrm{P}=2^{-k}\underset{k\to\infty}{\to}0$.

Пример интерактивной системы доказательства, основанной на задаче теории графов (1)

Графы G_0 и G_1 называются изоморфными, т.е. $G_0 \approx G_1$, если существует взаимно однозначное соответствие между их вершинами, при котором соединенным ребром вершинам в графе G_0 соответствуют соединенные вершины в графе G_1.

Задача проверки изоморфности графов не решаема за полиномиальное время.

Не упрощая задачи, можно предполагать, что G_0 и G_1 – графы на одном и том же множестве вершин N мощности m: $|N| = m$. $L = GNI = \{(G_0, G_1) | \forall G_0 \not\approx G_1\}$ – множество пар неизоморфных графов. P доказывает V утверждение $S = (G_0, G_1) \in GNI$.

Пример интерактивной системы доказательства, основанной на задаче теории графов (2)

	P		***V***
1		$\leftarrow$	Для $i=\overline{1,m}$ берет $\alpha_i \in \{0,1\}$ – случайный бит, создает изоморфную копию $G_{\alpha_i}' \approx G_{\alpha_i}$ путем случайной перестановки вершин: $G_{\alpha_i}' = \{(\pi(u),\pi(v)) \mid (u,v) \in E_{\alpha_i}\}$
2	Для $i=\overline{1,m}$ вычисляет $\beta_i \in \{0,1\}$ так, что: $\begin{cases} \beta_i = 0, если\left(G_{\alpha_i}' \approx G_0\right), \\ \beta_i = 1, если\left(G_{\alpha_i}' \approx G_1\right), \\ \beta_i - случ., если(G_0 \approx G_1), \text{ о} \\ \beta_i = 0, если\begin{pmatrix} G_{\alpha_i}' \not\approx G_0, \\ G_{\alpha_i}' \not\approx G_1 \end{pmatrix}, \end{cases}$ тправляет β_i проверяющему	$\rightarrow$	
3			Принимает доказательство тогда и только тогда, когда все биты совпали: для $\forall \alpha = \overline{1,m}$ $\beta_i = \alpha_i$.

Свойства интерактивных доказательств

Протокол между участниками *P* и *V* называется *интерактивным доказательством* для языка *L*, если *V* полиномиально ограничен, и выполнены следующие два условия:

1) для $\forall x \in L \;\; \mathrm{P}\{(P,V)_{(x)} = 1\} \geq 1 - \frac{1}{2^{n^C}}$ **, где *C=Const.*, *n* – число раундов протокола (т.е. вероятность принятия проверяющим доказательства истинного утверждения стремится к единице);**

2) для $\forall x \in L$ **и для** $\forall P' \neq P$ **(для любого другого участника, который действует не так, как честный участник) вероятность принятия проверяющим доказательства ложного утверждения исчезающе мала, т.е.** $\mathrm{P}\{(P',V)_{(x)} = 1\} \leq \frac{1}{2^{n^C}}$ **.**

Условие 1 называется *полнотой* (completeness), условие 2 – *корректностью* (soundness) доказательства. Класс языков, обладающих интерактивными системами доказательства, обозначается *IP*.

Теорема. **(*A.Shamir, A.Shen, 1990*) *IP=PSPACE*, т.е. класс задач, обладающих интерактивными системами доказательства, совпадает с классом задач, решаемых с полиномиальным объемом памяти.**

Доказательства с нулевым разглашением: постановка задачи (1)

Пусть задана интерактивная система доказательства $\langle P,V,S\rangle$. В определении интерактивной системы доказательства ранее не предполагалось, что *V* может быть противником (предполагалась только возможность существования нечестного участника P'). Но *V* может оказаться противником, который хочет выведать у *P* какую-либо новую полезную информацию об утверждении *S*. В этом случае *P* может не хотеть, чтобы это случилось в результате работы протокола интерактивной системы доказательства $\langle P,V,S\rangle$. Таким образом приходим к идее протокола доказательства с *нулевым разглашением* (zero-knowledge proof). Нулевое разглашение подразумевает, что в результате работы протокола интерактивной системы доказательства *V* не увеличит свои знания об утверждении *S*, или, другими словами, не сможет извлечь никакой информации о том, почему *S* истинно.

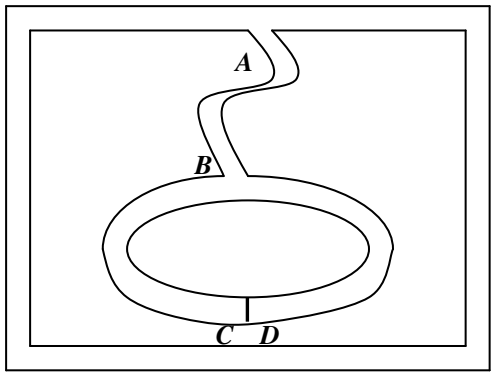
Как и ранее, в протоколе предварительно формулируется некоторое утверждение *S*, например, о том, что некоторый объект *w* обладает свойством *L*: $w \in L$. В ходе протокола *P* и *V* обмениваются сообщениями. Каждый из них может генерировать случайные числа и использовать их в своих вычислениях. В конце протокола *V* должен вынести свое окончательное решение о том, является ли *S* истинным или ложным.

Доказательства с нулевым разглашением: постановка задачи (2)

Цель *P* всегда состоит в том, чтобы убедить *V* в том, что *S* истинно, независимо от того, истинно ли оно на самом деле или нет, т.е. *P* может быть активным противником, а задача *V* – проверять аргументы *P*. Цель участника *V* заключается в том, чтобы вынести решение, является ли *S* истинным или же ложным. Как и ранее, *V* имеет полиномиально ограниченные вычислительные возможности, а именно время его работы ограничено некоторым полиномом от длины доказываемого утверждения: $t \le p(|w|)$. В силу этого он самостоятельно, без помощи *P*, не способен распознать истинность высказывания *S*. Вычислительные возможности *P* никак не ограничиваются.

«Задача о пещере Али-Бабы»

Это модельная задача, наглядно иллюстрирующая суть доказательств с нулевым разглашением. Имеется пещера, план которой показан на рисунке. Пещера имеет дверь с секретом между точками *C* и *D*. Каждый, кто знает волшебные слова, может открыть эту дверь и пройти из *C* в *D* или наоборот. Для всех остальных оба хода пещеры ведут в тупик.



Пусть *P* знает секрет пещеры. Он хочет доказать *V* знание этого секрета, не разглашая волшебные слова. Вот протокол их общения.

1. *V* находится в точке *A*.

2. *P* заходит в пещеру и добирается либо до точки *C*, либо до точки *D*.

3. После того, как *P* исчезает в пещере, *V* приходит в точку *B*, не зная, в какую сторону пошел *P*.

4. *V* зовет *P* и просит его выйти либо из левого, либо из правого коридора пещеры согласно желания *V*.

5. *P* выполняет это, открывая при необходимости дверь, если, конечно, он знает волшебные слова.

6. *P* и *V* повторяют шаги (1) – (5) *n* раз.

Если *P* не знает секрета двери, вероятность того, что *V* попросит его выйти из того же коридора, в который он вошел, равна $\frac{1}{2}$. После *n* раундов вероятность сократится до $\frac{1}{2^n}$.

Протокол доказательства изоморфизма графов

P **хочет доказать** ***V*** **изоморфизм графов** G_0 **и** G_1**. Пусть** $G_1 = \varphi(G_0): G_0 \approx G_1$**, где** φ **- преобразование изоморфизма.** m **– мощность множества** N **вершин графов.**

	P		***V***	
1	π - случайная перестановка вершин, вычисляет $H = \pi G_1$	$\rightarrow$		m раз
2		$\leftarrow$	$\alpha = \{0,1\}$-случ.	
3	Посылает преобразование ψ, такое что: $\psi = \begin{cases} \pi, если(\alpha = 1), \\ \pi \circ \varphi, если(\alpha = 0). \end{cases}$	$\rightarrow$		
4			Вычисляет граф ψG_α и сравнивает: $H \overset{?}{=} \psi G_\alpha$.	
5			Принимает доказательство тогда и только тогда, когда для $\forall m \quad H^{(m)} = \psi G_\alpha^{(m)}$.	

Протокол доказательства знания дискретного логарифма

Перед началом работы протокола задаются открытые величины: *p, q* – простые числа, такие, что $q|(p-1)$, элемент $g \in Z_p^*$, число *X*. Доказывающему *P* известна секретная величина $x : x \in Z_q, g^x = X$, знание которой он должен доказать *V*, не разглашая самой секретной величины.

	P		***V***
1	$r \in_R Z_q$ $M = g^r \pmod p$	$\rightarrow$	
2		$\leftarrow$	$R \in_R Z_q$
3	$m = r + xR \pmod q$	$\rightarrow$	
4			$g^m \stackrel{?}{=} X^R \cdot M \pmod p$

Протокол доказательства знания представления числа в базисе

Перед началом работы протокола задаются открытые величины, известные всем участникам: простые числа *p*, *q*, элементы $y, g_1, g_2, \ldots, g_k \in G_q$. Доказывающему *P* известны секретные величины $\alpha_1, \alpha_2, \ldots, \alpha_k \in Z_q : y = g_1^{\alpha_1} \cdot g_2^{\alpha_2} \ldots \cdot g_k^{\alpha_k}$, знание которых он должен доказать *V*, не разглашая самих этих величин.

	P		***V***
1	$r_1, r_2, \ldots, r_k \in_R Z_q$ $M = g_1^{r_1} \cdot g_2^{r_2} \cdot \ldots \cdot g_k^{r_k}$	$\rightarrow$	
2		$\leftarrow$	$R \in_R Z_q$
3	$m_i = r_i + \alpha_i R, i = \overline{1,k}$	$\rightarrow$	
4			$g_1^{m_1} \cdot g_2^{m_2} \cdot \ldots \cdot g_k^{m_k} \stackrel{?}{=} y^R \cdot M$

Доказательство знания представления множества чисел в соответствующих базисах

Перед началом работы протокола задаются открытые величины, известные всем участникам: простые числа *p,q*, элементы $y^{(j)}, g_1^{(j)}, g_2^{(j)}, \ldots, g_k^{(j)} \in G_q$ для некоторых *(j)*. Доказывающему *P* известны секретные величины $\alpha_1, \alpha_2, \ldots, \alpha_k \in Z_q$, такие, что для $\forall j$ $y^{(j)} = \left(g_1^{(j)}\right)^{\alpha_1} \cdot \left(g_2^{(j)}\right)^{\alpha_2} \cdot \ldots \cdot \left(g_k^{(j)}\right)^{\alpha_k}$, знание которых он должен доказать *V*, не разглашая самих этих величин.

	P		***V***
1	$r_1, r_2, \ldots, r_k \in_R Z_q$, для $\forall j$ $M^{(j)} = \left(g_1^{(j)}\right)^{r_1} \cdot \left(g_2^{(j)}\right)^{r_2} \cdot \ldots \cdot \left(g_k^{(j)}\right)^{r_k}$	$\rightarrow$	
2		$\leftarrow$	$R \in_R Z_q$
3	$m_i = r_i + \alpha_i R, i = \overline{1,k}$	$\rightarrow$	
4			для $\forall j$ $\left(g_1^{(j)}\right)^{m_1} \left(g_2^{(j)}\right)^{m_2} \cdot \ldots \cdot \left(g_k^{(j)}\right)^{m_k} \stackrel{?}{=}$ $\stackrel{?}{=} \left(y^{(j)}\right)^R \cdot M^{(j)}$

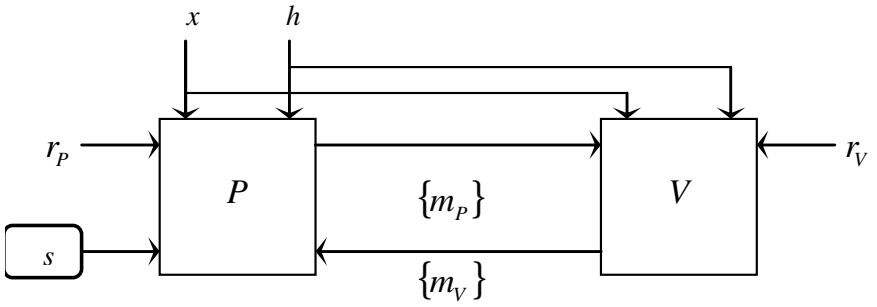
Структура протоколов доказательства с нулевым разглашением

В общем виде протокол интерактивного доказательства с нулевым разглашением состоит из четырех шагов:

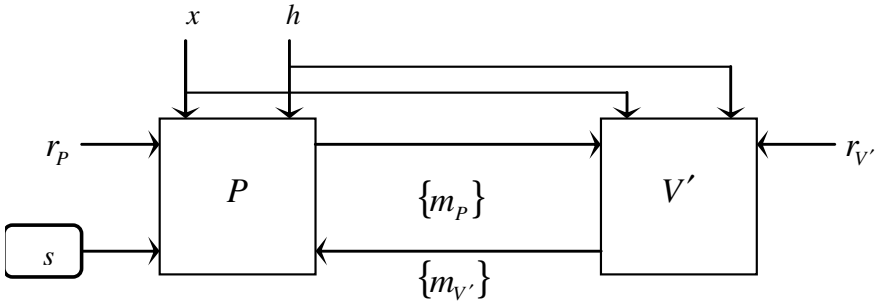
- **доказывающий передает проверяющему *W* – результат вычисления однонаправленной функции от секретной величины, знание которой он доказывает;**
- **проверяющий посылает ему случайный запрос;**
- **доказывающий отвечает на этот запрос, причем ответ зависит как от случайного запроса, так и от секретной величины, но из него вычислительно невозможно получить эту секретную величину;**
- **получая ответ, *V* проверяет его соответствие величине, переданной на первом шаге.**

	P	$S : x \in L$ – доказываемое утверждение, h – др. общедоступные параметры и величины, s – секретные данные доказывающего о том, почему S истинно, r – случ. число	***V***
1	r_P – случ., $W = f_1(x, r_P)$	$\rightarrow$	
2		$\leftarrow$	r_V – случ., $C = f_2(r_V)$
3	$R = f_3(C, x)$	$\rightarrow$	
4			$R \overset{?}{\approx} W$

Свойства доказательств с нулевым разглашением (1)



честный проверяющий



противник M

Пусть $\{m_P\},\{m_V\}$ – совокупность всех сообщений, передаваемых от *P* к *V* (соответственно от *V* к *P*), каждое из которых является случайной величиной, и таким образом, $\{x,h,r_V,\{m_P\},\{m_V\}\}=view_{P,V}(x,h)$ – это ансамбль случайных величин протокола, наблюдаемых извне (внешним наблюдателем), $\{x,h,r_{V'},\{m_P\},\{m_V\}\}=M_{V'}(x,h)$ – это ансамбль случайных величин, получаемых в результате работы полиномиального моделирующего алгоритма (simulator), который выполняется внешним наблюдателем (противником) самостоятельно.

Свойства доказательств с нулевым разглашением (2)

Если величины $view_{P,V}(x,h) \overset{C}{\approx} M_{V'}(x,h)$ ***вычислительно неразличимы*** **за полиномиальное время (т.е. не существует никакого алгоритма, который за полиномиальное время мог бы распознать эти два ансамбля случайных величин), то говорят, что протокол обеспечивает *вычислительно нулевое разглашение* (computationally zero-knowledge).**

Если величины $view_{P,V}(x,h) \approx M_{V'}(x,h)$ ***одинаково распределены*** **над множеством случайных величин, то говорят, что протокол обеспечивает *абсолютно нулевое разглашение* (perfect zero-knowledge).**

Система $\langle P,V,S \rangle$ **называется *интерактивной системой доказательства с нулевым разглашением* для языка *L*, если она:**

1) является интерактивной системой доказательства для языка *L* (т.е. обладает свойствами полноты и корректности);

2) обладает свойством нулевого разглашения.

Теорема 1. **(*Goldreich O., Krawchyk H.*) Последовательное выполнение двух протоколов с нулевым разглашением является протоколом с нулевым разглашением.**

Теорема 2. **(*Goldreich O., Krawchyk H.*) Параллельное выполнение протоколов с нулевым разглашением не обязательно приводит к протоколу с нулевым разглашением.**

Другие виды вероятностных доказательств

Среди всех протоколов доказательства с нулевым разглашением выделяют класс протоколов *доказательства знания* (*proof of knowledge*).

Например, доказательство знания чисел *p*, *q*, таких, что $p \cdot q = n$ есть доказательство знания, но доказательство того, что *n* – составное число, доказательством знания не является – это так называемое *доказательство обладания* (*proof of possession*).

Но доказательство знания не обязательно должно быть доказательством с нулевым разглашением, так как можно просто сообщить секрет другой стороне протокола: при этом сообщивший докажет знание секрета, но тем самым разгласит секрет. В различных приложениях криптографии, в частности, в протоколах аутентификации и в схемах электронных платежей, встречаются протоколы *доказательства знания с нулевым разглашением* (*zero-knowledge proof of knowledge – ZKPK*). Существуют специальные разновидности протоколов доказательства знания с нулевым разглашением: протоколы группового и «скрытого» доказательства знания и др.

Неинтерактивные доказательства с нулевым разглашением **(*non-interactive zero-knowledge proofs*) – однораундовые протоколы доказательства с нулевым разглашением, в которых доказывающий формирует, а проверяющий проверяет доказательство, пользуясь общей ссылочной строкой (common reference string), которая служит заменой случайного запроса проверяющего к доказывающему на шаге (2) обычного интерактивного протокола.**