Доказательства в криптографические протоколах

Вероятностные доказательства

Термин «вероятностные доказательства» объединяет класс криптографических протоколов, имеющих, как правило, вспомогательный характер, в которых одна из сторон с некоторой вероятностью убеждает другую сторону в справедливости некоторого утверждения.

В класс вероятностных доказательств включают: интерактивные системы доказательства, доказательства с нулевым разглашением знания, вероятностно-проверяемые доказательства и другие виды доказательств.

Интерактивные системы доказательства

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 ∈ 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 ложным. Как видим, интересы участников протокола P и V не совпадают.

Однако участник V имеет полиномиально ограниченные вычислительные возможности, а именно время его работы

ограничено некоторым полиномом от длины доказываемого утверждения:
t < =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:

если S истинно, P смог бы убедить V признать это;
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 из теории чисел

Зададимся натуральным числом *n*. Рассмотрим мультипликативную группу $Z_n^* = \{x < n; (x,n) = 1\}$. Обозначим $QR = \{(x,n) | x < n, (x,n) = 1, \exists y : y^2 \equiv x \bmod n\}$ – 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 $L = QNR = \{(x,n) | x < n, (x,n) = 1, \nexists y : y^2 \equiv x \bmod n\}$ – 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.

	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 $\forall (i = \overline{1,k})$ $c_i = b_i$.

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.**

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

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** $P = \frac{1}{2}$**. Следовательно, все** ***k*** **бит** $\{b_1,...,b_k\}$ **он сможет угадать лишь с вероятностью** $P = 2^{-k} \underset{k \to \infty}{\to} 0$**.**

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

1. Полнота. Если доказывающий знает утверждение, то он сможет убедить в этом проверяющего. (Т.е. вероятность принятия

проверяющим доказательства истинного утверждения стремится к единице при увеличении числа раундов протокола)

2. Корректность. Если доказывающий не знает утверждение, то он может обмануть проверяющего только с пренебрежимо малой вероятностью.

Если ввести третье утверждение - нулевое разглашение, то это будет интерактивное доказательство с нулевым разглашением.

3. Проверяющий, даже если он ведет себя нечестно, не узнает ничего кроме самого факта, что утверждение известно доказывающему.

Доказательства с нулевым разглашением (Zero-knowledge proof)

Представляет собой криптографический протокол, позволяющий одной из сторон (проверяющему) убедиться в том, что вторая сторона (доказывающая) знает какое-либо утверждение, при этом проверяющий не получает никакой другой информации о самом утверждении. Другими словами, А доказывает знание секрета, не разглашая самого секрета.

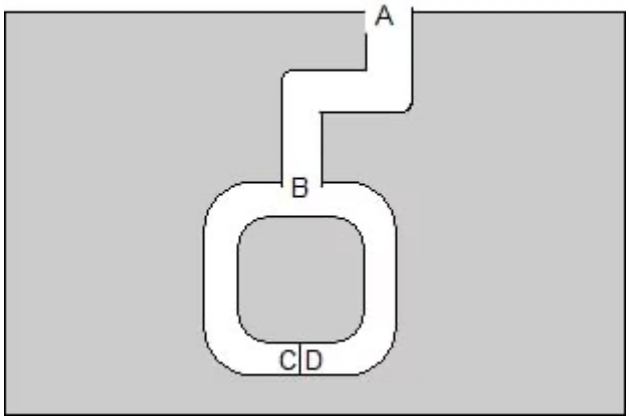
Использовать доказательства с нулевым знанием для доказательства идентичности было впервые предложено Уриелем Файгом, Амосом Фиатом и Ади Шамиром. В данном случае пользователь доказывает знание своего закрытого ключа, который в данном случае выступает в роли секрета, не раскрывая его. Таким образом, он доказывает свою идентичность.

Доказательство имеет форму интерактивного протокола. Это означает, что сторона В задает ряд вопросов доказывающему, которые если знает секрет, то ответит на все вопросы правильно. Если секрет стороне А неизвестен, но она хочет убедить в обратном

проверяющего, у нее есть некоторая вероятность (может быть 50 %, как в примерах ниже) ответить правильно на вопрос. Однако, после некоторого количества вопросов (10 — 20) проверяющий с достаточно высокой вероятностью убеждается в том, что доказывающий не знает секрет. При этом, ни один из ответов не дает никаких сведений о самом секрете.

Пещера нулевого знания

Хорошо поясняют доказательство с нулевым знанием Жан-Жак Кискатер и Луи Гиллу с помощью истории о пещере Али-Бабы (см. рисунок). Чтобы пройти сквозь пещеру, необходимо открыть дверь между C и D. Дверь открывается только тогда, когда кто-нибудь произносит волшебные слова. Пусть Пегги знает волшебные слова и хочет доказать это Виктору, не раскрывая самих слов.



Вот как происходит доказательство с нулевым знанием в данном случае:

1. Виктор находится в точке A.
2. Пегги проходит весь путь по пещере до двери либо по проходу C, либо по проходу D. Виктор не видит в какую сторону пошла Пегги. После того, как Пегги исчезнет в пещере, Виктор переходит в точку B.
3. Виктор кричит Пегги, чтобы она вышла из пещеры либо из левого

прохода, либо из правого прохода.
4. Пегги, при необходимости используя волшебные слова, чтобы отпереть дверь, выходит из пещеры из того прохода, из которого просил ее выйти Виктор.
5. Пегги и Виктор повторяют этапы 1-4 некоторое количество раз.

В случае когда Пегги не знает секрета, то она не сможет обмануть Виктора, если этапы доказательства (аккредитации) повторяются несколько раз подряд. Так как она может выйти только из того прохода, в который она зашла, в каждом раунде протокола вероятность угадать, с какой стороны Виктор попросит ее выйти, составляет 50 %. Соответственно, ее вероятность обмануть Виктора также равна 50 %. Однако, вероятность обмануть его в двух раундах составит уже 25 %, а в n раундах у нее есть только один шанс из 2^n. Виктор может уверенно предположить, что если все n (n=10-20) раундов доказательства Пегги правильны, то она действительно знает тайные слова, открывающие дверь между точками C и D.

Протокол Фиата-Шамира

Одним из наиболее известных протоколов идентификации личности с помощью доказательства с нулевым знанием является протокол, предложенный Амосом Фиатом и Ади Шамиром, стойкость которого основывается на сложности извлечения квадратного корня по модулю достаточно большого составного числа n, факторизация которого неизвестна.

Предварительно, перед самим доказательством доверенный центр T выбирает и публикует модуль достаточно большого числа n = p*q, разложить на множители которое трудно. При этом p, q – простые числа и держатся в секрете. Каждый пользователь A выбирает секретное s из интервала (1, n−1) взаимно простое с n. Затем вычисляется открытый ключ v = s^2 (mod n).

Полученное v регистрируется центром доверия в качестве открытого ключа пользователя A, а значение s является секретом A. Именно знание этого секрета s необходимо доказать A стороне B без его разглашение за t раундов. Каждая аккредитация состоит из следующих этапов:

1. A выбирает случайное r из интервала (1, n−1) и отсылает x = r^2 (mod n) стороне B.

2. B случайно выбирает бит e (0 или 1) и отсылает его A.

3. A вычисляет y = r*s^e (mod n) и отправляет его обратно к B.

4. Сторона B проверяет равенство y^2 ≡ x*v^e (mod n). Если оно верно, то происходит переход к следующему раунду протокола, иначе доказательство не принимается.

Выбор e из множества предполагает, что если сторона A действительно знает секрет, то она всегда сможет правильно ответить, вне зависимости от выбранного e. Допустим, что A хочет обмануть B, выбирает случайное r и отсылает x = r^2 / v, тогда если e=0, то A удачно возвращает B y = r, в случае же e=1, A не сможет правильно ответить, т.к. не знает s, а извлечь квадратный корень из v по модулю n достаточно сложно.

Вероятность того, что пользователь A не знает секрета s, но убеждает в обратном проверяющего B будет оцениваться вероятностью равной p = =2^(–t), где t – число аккредитаций. Для достижения высокой достоверности его выбирают достаточно большим (t = 20 – 40). Таким образом, B удостоверяется в знании A тогда и только тогда, когда все t раундов прошли успешно.

Для того, чтобы этот протокол корректно выполнялся, сторона A никогда не должна повторно использовать значение x. Если бы A поступил таким образом, а B во время другого цикла отправил бы A на шаге 2 другой случайный бит r, то B бы имел оба ответа A. После этого

B может вычислить значение s, и ему будет известен секретный ключ Алисы.

Ниже таблица с формальным описанием протокола

P – соответствует пользователю A

V – соответствует пользователю B

Предварительный этап			
P		***Центр доверия***	***V***
s: $(s,n)=1, 1\le s\le n-1$, $v=s^2 \pmod n$		p,q – бóльшие простые числа, $n=pq$	
n, v			
Рабочий этап			
	P		***V***
1	r – случайное число, $1\le r\le n-1$, $x=r^2 \bmod n$	→	
2		←	$e\in\{0,1\}$ – случайное число
3	$y=r\cdot s^e \pmod n$	→	
4			Если $(y=0)$, отклоняет доказательство, так как $r=0$. В противном случае $y^2 \stackrel{?}{\equiv} x\cdot v^e \pmod n$

Таким образом, 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.

Легко увидеть, что любую из схем электронной подписи легко и естественно можно преобразовать в протоколы интерактивной идентификации, заменяя хэш-код подписываемого сообщения или само сообщение заменяется на зарос проверяющего.

Неинтерактивный протокол — частный случай интерактивного, выполняемый за один раунд (посылка одного сообщения от доказывающего проверяющему).

Одна из моделей таких протоколов, когда 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.

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.

Протоколы аутентификации

Протокол аутентификации - криптографический протокол, в ходе которого одна сторона удостоверяется в идентичности другой стороны, вовлеченной в протокол, а также убеждается в том, что вторая сторона активна во время или непосредственно перед моментом приобретения доказательства.

В протоколе аутентификации участвуют две стороны: претендент (claimant - P), или доказывающий, и проверяющий (verifier - V). Последний уже предполагает некоторую ожидаемую идентичность

претендента, т. е. P не является для V совсем незнакомым лицом - его только нужно правильно выбрать из списка известных лиц. Цель V заключается в том, чтобы подтвердить предполагаемую идентичность претендента, т. е. что он в самом деле является P, а не кем-то иным. Проверяющий на выходе протокола аутентификации должен либо принять претендента как аутентичного, либо отвергнуть его как не соответствующего заявленной идентичности. Более строго, требования к протоколу аутентификации состоят в следующем:

1. **если P и V являются честными, V завершит протокол, приняв идентичность P;**
2. **V не может повторно использовать протокол, совершенный с P, для того, чтобы успешно деперсонифицировать P в протоколе с третьей стороной M**
3. **вероятность того, что любая сторона M, отличная от P, проведя протокол и играя роль P, может заставить V завершить протокол с принятием идентичности P, пренебрежимо мала;**
4. **предыдущие свойства остаются справедливыми, даже если между P и V совершено большое, но полиномиально ограниченное число сеансов протокола аутентификации, противник M участвовал в предыдущих сеансах выполнения протокола и несколько сеансов могли выполняться одновременно.**

Известны три принципиально разных способа аутентификации:
1. «Субъект знает» - претендент обладает некоторой информацией, которой нет у других субъектов компьютерной системы (паролями, цифровыми кодами, секретными ключами) и знание которой он демонстрирует в протоколах аутентификации.
«Субъект обладает» - претендент имеет некоторый физический предмет (магнитную карту, интеллектуальную карту, генератор паролей), который необходим для его участия в протоколе аутентификации и который выполняет для него криптографические преобразования информации.

«Субъект есть» - в протоколе проверяются некоторые признаки, характеризующие человеческую индивидуальность субъекта (иными словами, биометрические признаки: отпечатки пальцев, голос, рисунок радужной оболочки глаза и др.).
Криптографические протоколы реализуют первый подход - опознавание по логическому признаку. Очень часто при использовании технических средств становится возможной комбинация двух, а то и всех трех методов сразу. Одно из основных применений протоколов аутентификации - содействие контролю доступа к ресурсам компьютерных систем. Привилегия доступа к ресурсам обычно связывается с определенной идентичностью субъекта, что делает неизбежным предварительное выполнение протоколов аутентификации. Другие важные применения протоколов аутентификации - учет использования ресурсов компьютерной системы, распределение ключей криптографических систем и средств защиты информации.

Парольная аутентификация

Идея, лежащая в основе метода парольной аутентификации, чрезвычайно проста. Каждый субъект компьютерной системы имеет пароль - секрет, который он разделяет с системой. Демонстрация знания этого секрета (чаще всего путем разглашения самого пароля) принимается системой как подтверждение идентичности субъекта.

В качестве пароля обычно выбирается буквенная и (или) цифровая последовательность, которую пользователь легко может запомнить и при необходимости ввести по запросу системы. Различные парольные протоколы различаются по средствам, которыми хранится парольная информация внутри системы, и по методам ее проверки.
Можно выделить три основные угрозы протоколам парольной аутентификации: разглашение, прослушивание и угадывание пароля. Угрозы могут проявиться при осуществлении трех характерных видов

атак на парольные протоколы: при повторе паролей легальных пользователей злоумышленниками, полном переборе паролей и при словарной атаке на протокол.

На практике широко используются два типа протоколов парольной аутентификации: протоколы с фиксированными и с одноразовыми паролями.

Фиксированные пароли. Этот тип протоколов объединяет те из них, в которых пароль, предъявляемый претендентом системе, не меняется от одного сеанса выполнения протокола к другому. Пароль должен быть запоминаемым для человека (обычно не более 8-12 символов), время действия пароля ограничено разумными пределами, пароли должны периодически меняться. Для обеспечения достаточной стойкости протоколов аутентификации с фиксированными паролями используется ряд приемов:

хранение в компьютерной системе файлов паролей в защищенном режиме (с защитой от чтения-записи);

хранение в системе не самих паролей, а их образов, полученных как результат вычисления однонаправленной функции от пароля, взятого в качестве аргумента;

задание правил выбора паролей (минимальное количество символов, недопущение использования осмысленных слов, необходимость сочетания букв и цифр и т. п.), имеющих целью максимизировать энтропию пароля;

искусственное замедление процесса ввода пароля в систему с целью резкого увеличения времени на перебор паролей; выбор в качестве пароля осмысленного предложения (фразы) с последующим преобразованием посредством хеш-функции в короткое сообщение, которое обычно обладает большей энтропией, чем пароль такой же длины, выбираемый человеком;

добавление системой случайной величины к паролю перед обработкой его однонаправленной функцией - метод солтинга.

Все перечисленные методы лишь затрудняют или замедляют процесс доступа к паролю, его перебора или случайного угадывания. Ни один из них не решает проблемы защиты парольного протокола

радикально. Они обеспечивали вполне приемлемый уровень защиты в 70-80-е гг. XX в. с учетом тогдашнего уровня развития вычислительной техники и операционных систем. Сегодня перечисленные приемы простой аутентификации с фиксированными паролями используется, как правило, в не очень ответственных случаях или когда процесс доступа субъекта к системе необходимо максимально упростить (например, для входа пользователя в систему в массовых тиражируемых операционных системах семейств Windows или Linux). Разновидностью фиксированных паролей являются PIN-коды (от английских слов - Personal Identification Number). Это числовые пароли длиной от 4 до 8 десятичных цифр. Чаще всего они исполь-зуются в соединении с методом «обладания чем-либо»: обычно микропроцессорной пластиковой картой или картой с магнитной поло-сой. PIN-код обеспечивает второй уровень защиты на случай, если карта потеряна или украдена. Для защиты от полного перебора такого маленького ключевого пространства необходимы дополнительные меры: организационная и физическая защита. Например, банкомат может забрать у пользователя пластиковую карту или блокировать ее после нескольких подряд неудачных попыток ввода пароля.

Одноразовые пароли.

В протоколах этого типа каждый пароль используется только один раз, т. е. пароль является функцией некоторого аргумента. Известны три подхода к построению протоколов аутентификации с одноразовыми паролями:

1.Разделяемые списки одноразовых паролей. Пользователь и система имеют заранее определенную таблицу паролей, которую каждый из них хранит самостоятельно. При выполнении очередного сеанса протокола аутентификации выбирается пользователем и проверяется системой очередной пароль из этого списка.

2. Последовательно обновляемые одноразовые пароли. Первоначально пользователь и система имеют только один пароль,

условно с номером i. Затем пользователь создает и передает системе пароль под номером i-1, зашифрованный на ключе, вычисленном из i-го пароля. Следует заметить, что такой метод затруднительно реализовать при ненадежном канале связи (при возможности обрыва связи).

3. Последовательности одноразовых паролей, основанные на однонаправленных функциях. Этот метод наиболее эффективен по отношению к объему передаваемых данных. Примером является протокол Лампорта

Подготовительный этап:

1^0. Пользователь и система договариваются о числе N допустимых соединений (эта величина несекретна).

2^0. Клиент выбирает пароль W (128 бит и более), выполняет N раз последовательное хеширование пароля и передает системе цепочку результатов

$$H(W) = H^1(W)$$
$$H(H(W)) = H^2(W)$$
$$H(H(H(W))) = H^3(W)$$
$$\ldots\ldots\ldots\ldots$$
$$H(H(H(\ldots H(W)))) = H^N(W)$$

по секретному аутентичному каналу, защищенному от модификации (запись $H^k(W)$ означает результат последовательного вычисления хеш-функции k раз, а не возведения ее значения в степень k).

3^0.Система записывает число 1 в счетчик для подсчета числа сеансов аутентификации пользователя.

i-ый сеанс аутентификации

ё

1^0 .Система высылает пользователю число i.

2^0 .Пользователь выполняет $(N-i)$ раз хэширование пароля W и передает получившийся результат $H^{N-i}(W)$ системе.

3^0 . Система вычисляет $H(H^{N-i}(W)) = H^{N-i+1}(W)$ (еще раз хэширует присланное значение) и сверяет получившийся результат с хранящимся у нее значением $H^{N-i+1}(W)$.

4^0. При совпадении результата пользователь успешно подтверждает свою аутентичность, а система увеличивает счетчик сеансов аутентификаций на 1, т.е. теперь $i = i+1$.

Основной проблемой схемы Лэмпорта является активный злоумышленник (атака «человек посередине»). Очевидно, что в i - ом сеансе при отсутствии аутентификации системы перед пользователем до отправки ответа злоумышленник, может направить пользователю, якобы от имени системы, заведомо большее, чем текущее значение j счетчика (j > i). Тогда он может получить от клиента значение

H^{N-j} (W) и вычислять после этого любое значение из диапазона

Лабораторная N3

Группа 1

Осуществить аутентификацию с использованием симметричных криптосистем запрос-ответ на основе:

- **Протокола односторонней аутентификации с меткой времени**
- **Протокола односторонней аутентификации с использованием случайных чисел**
- **Протокола взаимной аутентификации с использованием случайных чисел**

Группа 2

Осуществить аутентификацию запрос-ответ, используя асимметричную криптосистему на основе:

- **Протокола односторонней аутентификации с меткой времени**
- **Протокола односторонней аутентификации с использованием случайных чисел**
- **Протокола взаимной аутентификации с использованием случайных чисел**

Группа 3

Реализовать протокол на основе доказательства с нулевым разглашением для аутентификации