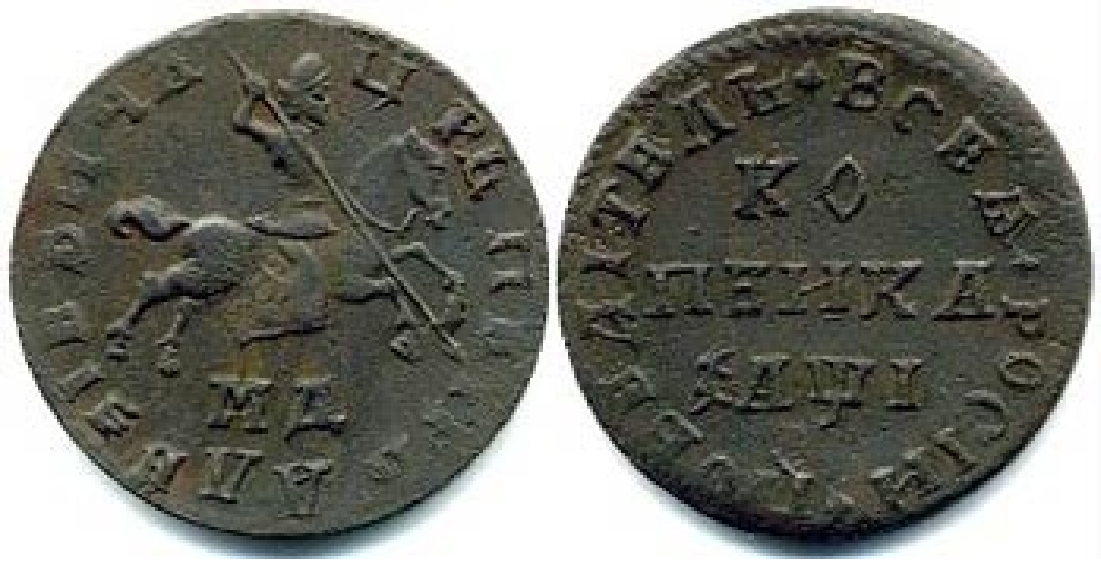
Подбрасывание монеты по телефону



У монеты две стороны. Одну, на которой чеканится герб, в народе называют **орлом**, другую – **решкой**. Первое слово, как всем известно, происходит от символа Российской империи – двуглавого орла, а вот со вторым всё не так ясно. **Решка** – это народное сокращение от «решето», «решётка». Дело в том, что на монетах не всегда печаталось их достоинство, выраженное в цифрах. Поначалу там чеканились слова, буквы которых располагались таким образом, что неграмотные люди принимали их за решето.

Кстати, и орёл не всегда был орлом, а сторону, противоположную решке, называли «копьём», поскольку на ней был изображён св. Георгий с копьём, пронзающим змея. *Копье аль решето?* (В. Даль).

Подбрасывание монеты по телефону

Подбрасывание монеты по телефону (англ. coinflippingbytelephone) — это эзотерический протокол, с помощью которого решается задача честного броска монеты между двумя участниками, находящимися на удалении друг от друга и при этом не доверяющими друг другу. Описание протокола было предложено американским ученым Мануэлем Блюмом в 1981 году, которое он опубликовал в своей статье «Подбрасывание монеты по телефону: протокол для решения нерешаемых задач».

Идея протокола честного броска монеты по телефону заключается в следующем. Алиса выбирает случайный (случайную последовательность) бит b, записывает его на листе бумаги, запирает этот лист в ящике, оставляя ключ от замка у себя, и посылает ящик Бобу. Не имея ключа, Боб не может добраться до содержимого ящика. Получив ящик, Боб выбирает случайный (случайную последовательность) бит c и посылает его Алисе. В ответ Алиса посылает Бобу ключ от ящика. Исходом подбрасывания монеты (серии бросков) будет бит $d = b \oplus c$.

Подбрасывание монеты по телефону

Подбрасывание монеты с помощью вручения бита

Эти ящики весьма напоминают блобы, предназначенный для вручения бита. Поэтому, когда Мануэлю Блюму встретилась проблема честного подбрасывания монетки по модему, он решил ее с помощью протокола вручения бита:

1. Алиса вручает случайный бит, используя какую-либо схему вручения бита, описанную выше (бросок).
2. Боб пытается отгадать бит Алисы (ответный бросок).
3. Алиса открывает свой бит Бобу. Если Боб угадал бит правильно, то результат броска «орел = 0», он выигрывает бросок, иначе – «решка = 1», выигрывает Алиса.

В общем случае нам необходим протокол с такими свойствами:

- Алиса должна «бросить монету» до того, как Боб попытается отгадать ее бит (загадать свой бит).
- У Алисы не должно быть возможности бросить монету повторно (изменить результаты своего броска), когда она узнает бит Боба.
- У Боба не должно быть возможности узнать результат броска Алисы до того, как он выскажет свою догадку.

Подбрасывание монеты по телефону

Подбрасывание монеты с помощью однонаправленных функций

1. $A \to B$:{Y}, где $Y = f(R_A)$, R_A – случайное число Алисы, f – однонаправленная функция общего пользования;
2. $B \to A$: {b}, где b – случайный бит Боба (Боб пытается отгадать чётность R_A);
3. $A \to B$:{R_A}, Алиса объявляет результат броска;
4. B: Боб проверяет что $f(R_A)$ совпадает с Y, полученным на проходе 1, далее, если чётности R_A и b совпадают, то результат «орел = 0», выигрыш Боба, если неверна – «решка = 1», выигрыш Алисы.

Подбрасывание монеты по телефону

Подбрасывание монеты с помощью однонаправленных функций

ЗАМЕЧАНИЕ 1. Надежность этого протокола опирается на однонаправленную функцию. Если Алиса всякий раз сумеет находить такие x и x', что x – четно, а x' – нечетно, но $y = f(x) = f(x')$, она сможет обманывать Боба в каждой игре.

ЗАМЕЧАНИЕ 2. Наименьший значащий бит $f(x)$ не должен коррелировать *с* x. *В* противном случае Боб сможет, по крайней мере, изредка, обманывать Алису. Например, если при четном значении x значение функции $f(x)$ в 75% случаев четное, у Боба есть преимущество. (Иногда наименьший значащий бит – не самый лучший выбор для практического использования, поскольку его вычисление может оказаться слишком простым).

Подбрасывание монеты по телефону

Подбрасывание монеты с помощью криптографии с открытым ключом

Приведенный ниже протокол может работать как с криптографией с открытым ключом, так и с симметричной криптографией. Единственное требование – коммутативность алгоритма, то есть: $D_{K_1}(E_{K_2}(E_{K_1}(M))) = E_{K_2}(M)$. Обычно этого свойства нет у симметричных алгоритмов, но справедливо для некоторых алгоритмов с открытым ключом (скажем, алгоритму RSA с идентичными модулями). Вот этот протокол:

1. A, B: Алиса и Боб генерируют пары открытый ключ/закрытый ключ. Если это система RSA, то они используют общий модуль. Все свои ключи держат в секрете друг от друга.
2. $A \rightarrow B$: $\{E_A(M_0), E_A(M_1)\}$, где M_0 = «ОрёлR_A», M_1 = «РешкаR_A», R_A – случайное число Алисы, сообщения $E_A(M_0)$ и $E_A(M_1)$, зашифрованные открытым ключом Алисы, Алиса отправляет в случайном порядке.
3. $B \rightarrow A$: $\{E_B(E_A(M_i))\}$, где $i = 0$ или 1 – это случайный выбор Боба из сообщений, полученных на шаге 2.

Подбрасывание монеты по телефону

Подбрасывание монеты с помощью криптографии с открытым ключом

Приведенный ниже протокол может работать как с криптографией с открытым ключом, так и с симметричной криптографией. Единственное требование – коммутативность алгоритма, то есть: $D_{K_1}(E_{K_2}(E_{K_1}(M))) = E_{K_2}(M)$. Обычно этого свойства нет у симметричных алгоритмов, но справедливо для некоторых алгоритмов с открытым ключом (скажем, алгоритму RSA с идентичными модулями). Вот этот протокол:

4. $A \to B$: $\{E_B(M_i)\}$, где $E_B(M_i) = D_A(E_B(E_A(M_i)))$ – это сообщение, полученное Алисой на шаге 3 и расшифрованное её закрытым ключом.
5. $B \to A$: $\{M_i\}$, где $M_i = D_B(E_B(M_i))$.
6. A: Алиса проверяет корректность своей случайной строки R_A в сообщении M_i, и убеждается в честности Боба.
7. Алиса и Боб открывают свои пары ключей с тем, чтобы каждая сторона убедилась в честности партнера на всех шагах.

Подбрасывание монеты по телефону

Подбрасывание монеты с помощью криптографии с открытым ключом

Этот протокол относится к числу *самодостаточных протоколов*. Любой участник может немедленно обнаружить мошенничество партнера на любом шаге.

ЗАМЕЧАНИЕ 1. Во всех приведенных протоколах броска честной монеты есть момент, когда один из участников знает результат броска раньше другого, но не может его изменить. Однако он может оттянуть раскрытие результата партнеру. Это явление известно как *бросок монеты в колодец*:Алиса стоит возле колодца, а Боб – немного в стороне. Боб бросает монету в колодец. Алиса может заглянуть в колодец и узнать результат, но не может изменить его. А Боб не может увидеть результат, пока Алиса не разрешит ему подойти к колодцу.

ЗАМЕЧАНИЕ 2. *Генерация ключей подбрасыванием монеты*. В практических приложениях протокол подбрасывания монеты так же используется для генерации сеансовых ключей. Протоколы броска монеты позволяют Алисе и Бобу генерировать случайный сеансовый ключ, причем такой, что ни один из них не сможет как-то влиять на его значение. А если Алиса и Боб еще и шифруют свои сообщения, сеансовый ключ не сумеет перехватить злоумышленник.

Доказательство с нулевым разглашением

Доказательство знания дискретного логарифма

Допустим, Пегги хочет доказать Виктору, что ей известно x, являющееся решением $A^x = B(\mathrm{mod}\ p)$, где p – простое число, а x – произвольное число, взаимно простое с $p - 1$. Числа A, B и p – общедоступны, а x хранится в секрете. Вот как Пегги, не раскрывая значения x, может доказать, что ей известно значение x:

1. $P \to V$: $\{h_1, h_2, \ldots, h_t\}$. Пегги генерирует t случайных чисел, $r_1, r_2, ..., r_t$, причем все r_i, меньше $p - 1$. Пегги вычисляет $h_i = A^{r_i} \mod p$ для всех значений i и посылает их Виктору.
2. P, V: Пегги и Виктор, воспользовавшись протоколом подбрасывания монеты, генерируют t случайных битов: $b_1, b_2, \ldots, b_t$.
3. $P \to V$: $\{s_1, s_2, ..., s_t\}$, где $s_i = \begin{cases} r_i, \text{ если } b_i = 0; \\ (r_i - r_j) \bmod (p-1), \text{ если } b_i = 1. \end{cases}$ Здесь и далее j – это наименьшее значение индекса, при котором $b_j = 1$.
4. V: Виктор проверяет, что $A^{s_i} \equiv \begin{cases} h_i (\mathrm{mod}\ p), \text{ если } b_i = 0, \\ h_i h_j^{-1} (\mathrm{mod}\ p), \text{ если } b_i = 1. \end{cases}$ Если проверка прошла успешно, то протокол продолжается.
5. $P \to V$: $\{Z\}$, где $Z = (x - r_j) \mod (p - 1)$.
6. V: Виктор проверяет, что $A^Z \equiv B h_j^{-1} (\mathrm{mod}\ p)$.

Вероятность удачного мошенничества Пегги равна 2^{-t}.

Доказательство с нулевым разглашением

Доказательство способности вскрытия RSA

Допустим, что Пегги знает закрытый ключ Кэрол и хочет убедить в этом Виктора. Однако она не хочет ни сообщать Виктору ключ, ни даже расшифровать для Виктора одно сообщение Кэрол. Пусть открытый ключ Кэрол – e, ее закрытый ключ – d, а модуль RSA – n.

1. P, V: Пегги и Виктор с помощью протокола подбрасывания монеты выбирают случайное значение k ($3 < k < n$) и вычисляют значение m из условия, что $km = e \pmod{n}$. Если m больше 3, протокол продолжается. В противном случае число k выбирается заново.
2. P, V: Пегги и Виктор с помощью протокола подбрасывания монеты генерируют случайный шифртекст C.
3. $P \rightarrow V$: $\{X\}$, где $X = (C^d)^k \bmod n$, Пегги вычисляет, используя закрытый ключ d Кэрол.
4. V: Виктор проверяет, что $X^m \bmod n = C$. Если это так, то он убеждается в правильности заявления Пегги.

Аналогичный протокол можно использовать для демонстрации способности вскрытия криптосистем, основанных на задаче дискретного логарифмирования.

Доказательство с нулевым разглашением

Доказательство того, что *n* является числом Блюма

Пока неизвестно никаких действительно практичных доказательств того, что $n = pq$, где p и q – простые числа, сравнимые с 3 по модулю 4. Однако если n имеет форму $p^r q^s$, где r и s нечетны, то у числа n все еще сохраняются свойства чисел Блюма, полезные для криптографии. И тогда существует доказательство с нулевым разглашением того, что n имеет указанную форму.

Предположим, что Пегги известно разложение на множители числа Блюма n, где n обладает рассмотренной выше формой. Вот как она может доказать Виктору, что n имеет такую эту форму.

1. $P \rightarrow V$: $\{u\}$, Пегги посылает Виктору число u, чей символ Якоби равен – 1 по модулю n.
2. P, V: Пегги и Виктор с помощью протокола подбрасывания монеты генерируют случайные биты: $b_1, b_2, \ldots, b_k$.
3. P, V: Пегги и Виктор с помощью протокола подбрасывания монеты выбирают случайные числа: $x_1, x_2, \ldots, x_k$.
4. $P \rightarrow V$: $\{a_i\}$. Для каждого $i = 1, 2, ..., k$ Пегги посылает Виктору квадратный корень по модулю n для одного из четырех чисел: x_i, $-x_i$, ux_i, $-ux_i$. Символ Якоби квадратного корня должен быть равен b_i.

Вероятность удачного мошенничества Пегги равна $1/2^k$.

Доказательство с нулевым разглашением

Впервые использовать доказательства с нулевым разглашением в целях аутентификации предложили Уриель Фейге (Uriel Feige), Амос Фиат (Amos Fiat) и Ади Шамир (Adi Shamir).

С помощью доказательства с нулевым разглашением, Алиса может доказать, что знает свой закрытый ключ не демонстрируя его, и, таким образом, доказать свою личность.

Уриэль Фейге (1959 Израиль) — профессор информатики и прикладной математики в институте Вейцмана. Вместе с Амосом Фиатом и Ади Шамиром принимал участие в разработке протокола аутентификации Фейга - Фиата - Шамира.

Доказательство с нулевым разглашением

Впервые использовать доказательства с нулевым разглашением в целях аутентификации предложили Уриель Фейге (Uriel Feige), Амос Фиат (Amos Fiat) и Ади Шамир (Adi Shamir).

С помощью доказательства с нулевым разглашением, Алиса может доказать, что знает свой закрытый ключ не демонстрируя его, и, таким образом, доказать свою личность.

Амос Фиат (род. 1 декабря 1956 г. Хайфа, Израиль) — профессор компьютерных наук в Тель-Авивском университете. Он известен своими работами в области криптографии, онлайн-алгоритмов и теории алгоритмических игр, получил докторскую степень в 1987 году в Институте науки Вейцмана под руководством Ади Шамира. После докторантуры у Ричарда Карпа и Мануэля Блюма в Калифорнийском университете в Беркли он вернулся в Израиль, заняв должность преподавателя в Тель-Авивском университете.

Доказательство с нулевым разглашением

При реализации протоколов аутентификации на основе доказательства с нулевым разглашением возможны следующие атаки посредника.

1. **Проблема гроссмейстера**

Алиса бросает вызов Гарри Каспарову и Анатолию Карпову, предлагая сыграть в одно время, в одном месте, но в разных комнатах с Карповым – черными фигурами, а с Каспаровым – белыми. Гроссмейстеры ничего не знают друг о друге, думают, что играют с Алисой, в то время как играют друг с другом через посредника Алису, которая перемещается между этими комнатами.

2. **Мошенничество мафии**

Предположим, Алиса закусывает в ресторане мафии «Обеды у Боба». Кэрол делает покупки в дорогом ювелирном магазине «Торговый Дом Дейва». Боб и Кэрол – мафиози, сообщающиеся по секретному радиоканалу. Алиса и Дэйв даже не подозревают обман. Когда Алиса приготовится доказать свою личность Бобу и оплатить счет, Боб дает знать Кэрол, по сути, Алиса доказывает свою личность Дэйву, а участие в протоколе Боба и Кэрол ограничивается передачей сообщения туда и обратно. По завершению протокола Алиса докажет свою личность Дэйву и заплатит за дорогие бриллианты, а Кэрол скроется с ними.

3. **Обман, выполненный террористами**

В этом случае Кэрол играет роль известной террористки, которой Алиса помогает въехать в страну. Дэйв – офицер-пограничник. Алиса и Кэрол сообщаются по секретному радиоканалу. Когда Дэйв задает Кэрол вопросы, предусмотренные протоколом с нулевым разглашением, Кэрол адресует их Алисе, та отвечает на вопросы и Кэрол повторяет их Дэйву. По существу, свою личность Дэйву доказывает Алиса, а Кэрол выступает в роли канала связи. По завершению протокола Дэйв уверен, что Кэрол – это Алиса, и разрешает ей въезд в страну.

Доказательство с нулевым разглашением

Успех атак, описанных выше, целиком зависит от секретного радиоканала. Поэтому есть следующие технические и организационные способы предотвращения этих атак.

1) Соответственно, один из путей их предотвращения — проводить процедуры идентификации в «клетке Фарадея», которая блокирует радиоволны.

2) Чтобы решить проблему гроссмейстера, можно заставить Алису не вставать с места до окончания партии или отслеживать её перемещения.

3) Томас Бет (Thomas Beth) и Иво Десмедт (Yvo Desmedt) предложили решение, в котором используются точные часы, чтобы у мошенников не оставалось времени для обмена сообщениями.

Томас Бет (род. 16 ноября 1949 года в Ганновере; † 17 августа 2005 года в Карлсруэ) – немецкий математик, который занимался информатикой и комбинаторикой. Томас Бет изучал математику (а также физику и медицину) в Геттингенском университете с 1968 по 1973 год. Затем он получил стипендию DAAD в Университете штата Огайо в 1973/74 году и с 1974 года научным сотрудником Университета Эрланген-Нюрнберг, где он получил докторскую степень по математике в 1978 году под руководством Конрада Якобса. В 1984 году он получил там степень хабилитации по информатике, а в 1984 году стал профессором Королевского Холлоуэйского колледжа Лондонского университета, где он возглавил факультет информатики и статистики и создал рабочую группу по криптографии. В 1985 году он стал профессором Университета Карлсруэ (TH), где он был соучредителем (и представителем) Института алгоритмов и когнитивных систем. В 1988 году он был основателем и директором Европейского института безопасности систем (EISS), а в начале (1982) организовал международные конференции по криптографии в Бург-Фойерштайн, из которых позже возникли конференции Eurocrypt.

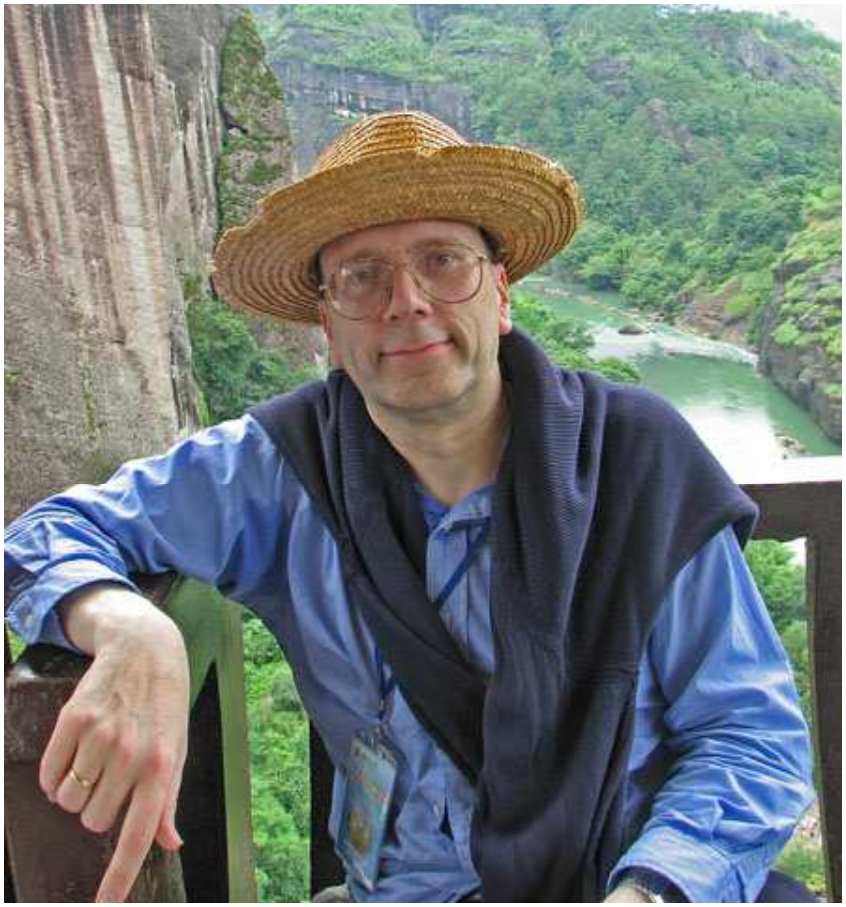
Доказательство с нулевым разглашением

Успех атак, описанных выше, целиком зависит от секретного радиоканала. Поэтому есть следующие технические и организационные способы предотвращения этих атак.

1) Соответственно, один из путей их предотвращения — проводить процедуры идентификации в «клетке Фарадея», которая блокирует радиоволны.

2) Чтобы решить проблему гроссмейстера, можно заставить Алису не вставать с места до окончания партии или отслеживать её перемещения.

3) Томас Бет (Thomas Beth) и Иво Десмедт (Yvo Desmedt) предложили решение, в котором используются точные часы, чтобы у мошенников не оставалось времени для обмена сообщениями.



Иво Г. Десмедт (1956 г.) - заслуженный профессор Джонссона Техасского университета в Далласе, а также заведующий кафедрой информационных коммуникационных технологий в Университетском колледже Лондона. Он был пионером пороговой криптографии и является научным сотрудником Международной ассоциации криптологических исследований. Он также сделал важные наблюдения, которые использовались при криптоанализе ранцевых криптосистем Меркла – Хеллмана, и обнаружил свойства стандарта шифрования данных, которые использовали Эли Бихам и Ади Шамир, когда они изобрели дифференциальный криптоанализ.