КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ

Возможности криптографии используются в реальных компьютерных системах:

- заключение коммерческих сделок в режиме удаленного взаимодействия участников
- осуществление денежных расчетов по сети
- проведение выборов по компьютерным сетям
- многое другое

Криптографические алгоритмы способны обеспечивать надежность значительно более высокую, чем традиционные механизмы.

Ментальный покер

Возникает задача проведения честной игры в карты, когда партнеры находятся далеко друг от друга, но связаны компьютерной сетью.

Далее рассмотрим предельно упрощенную постановку задачи, где участвуют всего
2 игрока и всего 3 карты
(обобщения на другие случаи очевидны).

Задача ставится следующим образом. Имеются два игрока Алиса и Боб и три карты α, β, γ. Необходимо раздать карты следующим образом: Алиса должна получить одну карту, Боб — также одну, а одна карта должна остаться в прикупе. При этом необходимо, чтобы:

1) каждый игрок мог получить с равными вероятностями любую из трех карт α, β или γ, а одна карта оказалась в прикупе;

2) каждый игрок знал только свою карту, но не знал карту противника и карту в прикупе;

3) в случае спора возможно было пригласить судью и выяснить, кто прав, кто виноват;

4) при раздаче карт с помощью компьютерной сети никто не знал, кому какая карта досталась (хотя раздача происходит по открытой линии связи и Ева может записать все передаваемые сообщения).

Протокол, позволяющий организовать такую раздачу карт, удобно разбить на два этапа.

Предварительный этап (для выбора параметров протокола):

Участники выбирают несекретное большое простое число p. Затем Алиса выбирает случайно число c_A, взаимно простое с $p-1$, и вычисляет по обобщенному алгоритму Евклида число d_A, такое, что

$$c_A d_A \bmod (p-1) = 1. \tag{5.1}$$

Независимо и аналогично Боб находит пару c_B, d_B, такую, что

$$c_B d_B \bmod (p-1) = 1. \tag{5.2}$$

Эти числа каждый игрок держит в секрете. Затем Алиса выбирает случайно три (различных) числа $\hat{\alpha}$, $\hat{\beta}$, $\hat{\gamma}$ в промежутке от 1 до $p-1$, в открытом виде передает их Бобу и сообщает, что $\hat{\alpha}$ соответствует α, $\hat{\beta}$ — β, $\hat{\gamma}$ — γ (т. е., например, число 3756 соответствует тузу и т.д.).

Основной этап (пошаговое описание):

Шаг 1. Алиса вычисляет числа

$$u_1 = \hat{\alpha}^{c_A} \bmod p,$$
$$u_2 = \hat{\beta}^{c_A} \bmod p,$$
$$u_3 = \hat{\gamma}^{c_A} \bmod p$$

и высылает u_1, u_2, u_3 Бобу, предварительно перемешав их случайным образом.

Шаг 2. Боб получает три числа, выбирает случайно одно из них, например u_2, и отправляет его Алисе по линии связи. Это и будет карта, которая достанется ей в процессе раздачи. Алиса, получив это сообщение, может вычислить

$$\hat{u} = u_2^{d_A} \bmod p = \hat{\beta}^{c_A d_A} \bmod p = \hat{\beta}, \tag{5.3}$$

т.е. она узнает, что ей досталась карта β (можно и не вычислять (5.3), так как она знает, какое число u_i какой карте соответствует).

Шаг 3. Боб продолжает свои действия. Он вычисляет для оставшихся двух чисел

$$v_1 = u_1^{c_B} \bmod p, \tag{5.4}$$

$$v_3 = u_3^{c_B} \bmod p. \tag{5.5}$$

С вероятностью 1/2 он переставляет эти два числа и отправляет Алисе.

Шаг 4. Алиса выбирает случайно одно из полученных чисел, например v_1, вычисляет число

$$w_1 = v_1^{d_A} \bmod p \tag{5.6}$$

и отправляет это число обратно к Бобу. Боб вычисляет число

$$z = w_1^{d_B} \bmod p \tag{5.7}$$

и узнает свою карту (у него получается $\hat{\alpha}$). Действительно,

$$z = w_1^{d_B} = v_1^{d_A d_B} = u_1^{c_B d_B d_A} = \hat{\alpha}^{c_A c_B d_A d_B} = \hat{\alpha} \bmod p.$$

Карта, соответствующая v_2, остается в прикупе.

Утверждение 5.1. *Описанный протокол удовлетворяет всем свойствам честной раздачи карт.*

Идея доказательства:

Алиса перемешивает числа u_1, u_2, u_3 перед отправкой к Бобу. Затем Боб выбирает одно из этих чисел, не зная, какое число какой карте соответствует.

Если Боб выбирает карту случайно, обеспечивается то, что Алиса получает любую из карт с вероятностью **1/3**.

Аналогично, если Алиса выбирает одну из оставшихся двух карт случайно с равными вероятностями, то Боб также получает любую из трех карт с вероятностью **1/3**.

Очевидно, что при этих условиях и в прикупе каждая из карт может оказаться с вероятностью **1/3**.

Если Алиса или Боб будут нарушать некоторые требования протокола, то это может быть использовано им во вред.

Поэтому каждый участник заинтересован в точном выполнении всех правил.

Проверим это, считая, что игра повторяется многократно.

Предположим, что Алиса не перемешивает карты $\boldsymbol{u_1}$, $\boldsymbol{u_2}$, $\boldsymbol{u_3}$ а всегда посылает их в одной и той же последовательности или руководствуется каким-либо другим простым правилом.

Если раздача карт выполняется несколько раз, то Боб может использовать это в своих интересах (например, он всегда будет отправлять Алисе самую младшую карту и в каждом случае будет знать, какая карта ей досталась), т.е. Алисе выгодно перемешивать карты.

Аналогично, можно проверить, что при необходимости выбора каждому игроку лучше выбирать карту случайно, с равными вероятностями.

<u>Проверим выполнение второго требования, предъявляемого к честной раздаче карт.</u>

Когда Боб выбирает число u_i, соответствующее карте Алисы (шаг 2), он не знает секретное c_A, следовательно, он не может узнать, какое u_i какой карте соответствует, а вычисление c_A по u_i эквивалентно задаче дискретного логарифмирования (и практически невозможно при больших p).

Когда Алиса выбирает карту для Боба, а он для нее, никто из них не может определить достоинство этой карты, так как оно зашифровано при помощи либо c_A, либо c_B.

Ни Алиса, ни Боб не могут знать, какая карта осталась в прикупе, так как соответствующее число имеет вид $\boldsymbol{a^{c_A c_B}}$ (см. (5.4) и (5.5)).

Алиса не знает $\boldsymbol{d_B}$, а Боб не знает $\boldsymbol{d_A}$.

Проверим третье свойство.

В случае возникновения спора судья может повторить все вычисления по записанным предаваемым числам и выяснить, кто прав.

Проверим четвертое свойство.

По линии связи передаются числа $\boldsymbol{u_1}$, $\boldsymbol{u_2}$, $\boldsymbol{u_3}$, $\boldsymbol{v_1}$, $\boldsymbol{v_2}$, $\boldsymbol{v_3}$ и $\boldsymbol{w_1}$.

Каждое из них может быть представлено в виде $\boldsymbol{a^x \; mod \; p}$, где $\boldsymbol{x}$ неизвестно Еве.

Мы знаем, что нахождение $\boldsymbol{x}$ — задача дискретного логарифмирования, которая практически неразрешима. Значит Ева ничего не может узнать.

П р и м е р 5.1. Пусть Алиса и Боб хотят честно раздать три карты: тройку (α), семерку (β) и туза (γ). (Точнее, обычно в криптографии предполагается, что никто из них не хочет быть обманутым. Большей «честности» от них не ожидают.) Пусть на предварительном этапе выбраны следующие параметры:

$$p = 23, \quad \hat{\alpha} = 2, \quad \hat{\beta} = 3, \quad \hat{\gamma} = 5.$$

Алиса выбирает $c_A = 7$, Боб выбирает $c_B = 9$.

Найдем по обобщенному алгоритму Евклида d_A и d_B: $d_A = 19$, $d_B = 5$.

Шаг 1. Алиса вычисляет

$$u_1 = 2^7 \bmod 23 = 13,$$
$$u_2 = 3^7 \bmod 23 = 2,$$
$$u_3 = 5^7 \bmod 23 = 17.$$

Затем она перемешивает u_1, u_2, u_3 и высылает их Бобу.

Шаг 2. Боб выбирает одно из полученных чисел, пусть, например, выбрано число 17. Он отправляет число 17 к Алисе. Она знает, что число 17 соответствует карте γ, и, таким образом, ее карта при раздаче — туз.

Шаг 3. Боб вычисляет

$$v_1 = 13^9 \bmod 23 = 3,$$
$$v_2 = 2^9 \bmod 23 = 6$$

и отправляет эти числа к Алисе, возможно, переставив их местами.

Шаг 4. Алиса получает числа 3 и 6, выбирает одно из них, пусть это будет 3, и вычисляет число

$$w_1 = 3^{19} \bmod 23 = 6.$$

Это число она отправляет Бобу, который вычисляет число

$$z = 6^5 \bmod 23 = 2$$

и узнает свою карту α, т.е. ему досталась тройка. В прикупе осталась семерка, но ни Алиса, ни Боб этого не знают. Ева же, следившая за всеми передаваемыми сообщениями, не может ничего узнать в случае большого p.

Честная карточная игра по сети с множеством участников

Пусть есть колода K из $|K|$ карт (для удобства будем считать, что все карты натуральные попарно различные числа, такое сопоставление можно легко ввести для любой реальной колоды из 52 карт, если, например, сопоставить картам числа в диапазоне от 2 до 53).

В игре участвуют $n \leq |K|$ игроков.

Необходимо раздать каждому игроку по $m_i, 1 \leq i \leq n, \sum_{i=1}^{n} m_i \leq |K|$ карт таким образом, чтобы никто из игроков не мог знать карты другого.

Сговоры между любым подмножеством игроков не должны влиять на честность раздачи карт.

Формируется большое простое число P (для большей надёжности это должно быть число Софи Жермен, то есть $P = 2Q + 1$, где P, Q - простые числа).

Каждый игрок формирует два секретных ключа $1 < C_i, D_i < P - 1$, $1 \leq i \leq n$, такие, что $C_i D_i \, mod \, (P - 1) = 1$.

Формируется колода

$$K = \{k_1, k_2, \dots, k_{|K|} | k_i \in \{2, P - 1\}, k_i \neq k_j, i \neq j\}.$$

После получения исходных параметров можно приступить к раздаче карт, которая выполняется по следующему алгоритму:

1. Шифрование колоды:
   Каждый игрок по очереди шифрует все карты колоды при помощи своего ключа C и перемешивает их, после чего передаёт колоду следующему игроку. Опишем указанные действия для i-го игрока:

$$K_{1..i} = shuffle\left(K_{1..i-1}^{C_i} \, mod \, P\right)$$

Здесь функция $shuffle()$ случайным образом перемешивает карты в колоде (переставляет элементы массива), а $K_{1..i-1}$ – это колода, зашифрованная и перемешанная по очереди всеми игроками от 1 до $i-1$. Так как колода K является множеством, то распишем подробнее: $K^C mod\ P = \{k_1^C mod\ P, \ldots, k_{|K|}^C mod\ P\}$

2. После первого шага получается колода, зашифрованная и перемешанная всеми игроками по очереди.

Теперь любой игрок (например, тот, который шифровал последним) может раздать всем остальным игрокам карты в любом порядке.

Так как на каждом шаге осуществлялось случайное перемешивание, то карты находятся уже в произвольном порядке и можно раздавать их подряд, в последовательном порядке, начиная с первой карты.

3. Теперь у каждого игрока на руках находятся $m_i, 1 \leq i \leq n$ карт, зашифрованных всеми игроками. Для того, чтобы узнать свои карты i-й игрок должен передать свои карты по очереди каждому игроку, чтобы те их расшифровали при помощи своих ключей D. Собственный ключ игрок использует в последнюю очередь.

Опишем процесс для одной карты k i-го игрока при помощи псевдокода:

```
FOR j = 1..n DO
  IF j ≠ i THEN
   k = k^{D_j} mod P
  FI
OD
```

$$k = k^{D_i} mod\ P$$

Для того, чтобы обезопасить протокол от попытки подмены карты каким-либо игроком в процессе игры, все пункты алгоритма записываются в лог, а после окончания игры каждый игрок публикует свои ключи C, D.

Таким образом, любой игрок, имея записи процесса раздачи и все ключи, может проверить, что все данные корректны и ни на каком этапе не произошло подмены.