Криптографическая защита информации

Лекция 6

Ментальный покер

Проблема

Раздать карты игрокам, которые находятся далеко друг от друга.

1. Причём каждый из них не доверяет другому;
2. Существует враг, готовый перехватить передаваемую по незащищенному каналу связи информацию.

Требования к протоколу раздачи карт

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 условии раздачи 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).

Предварительный этап (выбор параметров)

Предварительный этап необходим 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 $[1, p-1]$, 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.).

Шаг 1

Шаг 1. Алиса вычисляет числа

$$\begin{aligned} u_1 &= \hat{\alpha}^{c\wedge} \bmod p, \\ u_2 &= \hat{\beta}^{c\wedge} \bmod p, \\ u_3 &= \hat{\gamma}^{c\wedge} \bmod p \end{aligned}$$

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

Шаг 2

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

$$\hat{u} = u_2^{d_\wedge} \bmod p = \hat{\beta}^{c_\wedge d_\wedge} \bmod p = \hat{\beta}, \qquad (5.3)$$

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

Шаг 3. Боб продолжает свои действия. Он вычисляет два оставшихся числа

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

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

Затем он отправляет эти числа Алисе.

Шаг 4

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.

Пример (выбор параметров)

Пример 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: $d_A = 19$, $d_B = 5$.

Пример (шаги 1-3)

Шаг 1: Алиса вычисляет

$$\begin{aligned} u_1 &= 2^7 \bmod 23 = 13, \\ u_2 &= 3^7 \bmod 23 = 2, \\ u_3 &= 5^7 \bmod 23 = 17. \end{aligned}$$

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

$$\begin{aligned} v_1 &= 13^9 \bmod 23 = 3, \\ v_2 &= 2^9 \bmod 23 = 6 \end{aligned}$$

и отправляет эти числа к Алисе.

Шаг 4

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.

Литература

Рябко, Фионов.

Глава 5, параграфы 5.1.

Задание

1. Реализовать протокол ментального покера для раздачи карт.