Фролов Дмитрий Сергеевич
студент
Филимонов Антон Юрьевич
студент
Кротова Елена Львовна
канд. физ.-мат. наук, доцент
ФГБОУ ВПО «Пермский национальный исследовательский политехнический университет»
г. Пермь, Пермский край

ПРОТОКОЛ РАЗДАЧИ ТРЕХ КАРТ ДЛЯ ДВУХ УЧАСТНИКОВ

***Аннотация**: в статье рассмотрен криптографический протокол и его стойкость, а также приведены наглядные примеры его использования.*

***Ключевые слова**: криптографический протокол, криптостойкость.*

Начнем с того, что криптографический протокол – это такая процедура взаимодействия двух или более абонентов с использованием криптографических методов, в результате которой абоненты достигают своей определенной цели.

Рассмотрим довольно простой, но надежный протокол раздачи карт, в котором участвуют два игрока – A и B. Так же мы имеем три карты, которые нам и нужно раздать – α, β, γ.

Переменные протокола:

p – большое простое число, которое известно всем участникам;

α, β, γ – целые числа, которые соответствуют разным картам (к примеру, α соответствует даме треф, β – тузу червей, γ – королю червей).

Переменные участника A:

$c_A \in Z_p$ – случайное число, при этом НОД$(c_A, p\text{-}1) = 1$;

$d_A \in Z_p$: $c_A d_A \equiv 1(mod\ p\text{-}1)$. Пара (c_A, d_A) – секретный ключ A.

Переменные участника B:

$c_B \in Z_p$ – случайное число, при этом НОД$(c_B, p\text{-}1) = 1$;

$d_B \in Z_p$: $c_B d_B \equiv 1(mod\ p\text{-}1)$. Пара (c_B, d_B) – секретный ключ B [1, с. 68]

Реализация протокола раздачи карт выполняется в несколько шагов:

1. $A \to B$: $u_1 = \alpha^{c_A} \, mod \, p$,

$u_2 = \beta^{c_A} \, mod \, p$,

$u_3 = \gamma^{c_A} \, mod \, p$,

после расчетов A должен случайным образом перемешать числа;

2. $B \to A$: u_i, где $i \in \{1; 2; 3\}$ – случайное число;

3. $B \to A$: $v_1 = u_j^{c_B} \, mod \, p$,

$v_2 = u_k^{c_B} \, mod \, p$,

где $\{j, k\} = \{1,2,3\}/\{i\}$. Перед отправкой эти числа также случайным образом перемешиваются;

4. $A \to B$: $w_1 = v_s^{d_A} \, mod \, p$,

где s случайно выбирается из {1, 2};

5. A: вычисляет $x = u_i^{d_A} \, mod \, p$;

6. B: вычисляет $y = w_1^{d_B} \, mod \, p$.

В результате реализации протокола у игрока A будет на руках карта x, у B – карта y, и в прикупе будет лежать карта z, закрытая маскирующими коэффициентами c_A и c_B. Причем $\{x, y, z\} = \{\alpha, \beta, \gamma\}$.

Разберем поподробнее, что происходит на каждом шаге протокола, для этого обратимся к Алисе (A) и Бобу (B).

Шаг 1. A перекрывает колоду своим маскирующим коэффициентом c_A и, перемешав ее, передает B.

Шаг 2. B берет из колоды и возвращает A случайную карту (можно сказать, что игрок В возвращает случайную карту, т.к. он не видит, какие карты у него в руках).

Шаг 3. B перекрывает колоду своим маскирующим коэффициентом c_B и, перемешав ее, отдает A, в следствие чего на каждой карте колоды стоит два маскирующих коэффициента – c_A и c_B.

Шаг 4. A забирает из колоды и отдает B случайную карту, перед этим сняв с этой карты свой маскирующий коэффициент, а колоду кладет в прикуп.

Шаг 5. A снимает со своей карты свой маскирующий коэффициент и узнает значение розданной ему карты.

Шаг 6. B узнает значение своей карты.

После выполнения протокола, в прикупе остается карта, которая закрыта двумя маскирующими коэффициентами.

Стоит заметить, что все условия «честной» раздачи карт выполнены. Действительно, в раздаче принимают участие все игроки. Каждый игрок при раздаче видит перед собой колоду, закрытую маскирующим коэффициентом другого игрока. В прикупе же лежит карта, закрытая двумя маскирующими коэффициентами. Восстановить значения карт – значит решить задачу нахождения дискретного логарифма в конечном поле. Чтобы за полиномиальное время восстановить значение карт, нужно их угадать. Но вероятность такого угадывания слишком мала. Сдаваемые карты и колода передаются по каналу связи только в зашифрованном (закрытом маскирующими коэффициентами) виде.

Если все значения, передаваемые по каналам связи и карты, находящиеся у A и B, будут записаны, то арбитр, приглашенный рассудить, не было ли мошенничества со стороны игроков, может восстановить все действия протокола и узнать, на каком шаге и кем он был нарушен.

Заметим, что игрокам выгоднее придерживаться протокола, чем нарушать его. Действительно, единственная возможность для игрока A нарушить протокол так, чтобы это нельзя было отследить, это не перемешивать колоду при раздаче. Но такие действия позволят В узнать, где какая карта находится. То же самое относится к действиям В [1, с. 70]

Стойкость данного протокола основывается в первую очередь на сложности задачи нахождения дискретного логарифма в конечном поле.

Рассмотрим конкретный пример.

Пусть $p = 31$, $\alpha = 3$, $\beta = 20$, $\gamma = 6$.

$c_A = 7$, тогда с помощью расширенного алгоритма Евклида, A находит $d_A = 13$.

$c_B = 11$, тогда с помощью расширенного алгоритма Евклида, B находит $d_B = 11$.

1. A: вычисляет $3^7 mod\ 31 = 17, 20^7\ mod\ 31 = 18, 6^{\ 7} mod\ 31 = 6$;

$A \to B$: перемешанную колоду: $(6, 17, 18)$;

2. $B \to A$: 18;

3. B: вычисляет $6^{11} mod\ 31 = 26, 17^{11}\ mod\ 31 = 22$;

$B \to A$: перемешанную колоду $(26, 22)$;

4. A: выбирает карту из колоды ($s = 2$) и вычисляет $22^{13} mod\ 31 = 13$;

$A \to B$: 13;

5. A: вычисляет свою карту, сданную на шаге 2: $18^{13} mod\ 31 = 20 = \beta$;

6. B: вычисляет свою карту, сданную на шаге 4: $13^{11}\ mod\ 31 = 3 = \alpha$.

Сняв маскирующие коэффициенты с карты, оставшейся в прикупе, обнаруживаем, что $(26^{13})^{11} mod\ 31 = 6 = \gamma$.

Отметим, что не рекомендуется использовать для протокола раздачи карт криптосистему RSA, поскольку она дает некоторую утечку информации. Ведь если число является квадратом, то и в зашифрованном RSA виде оно также будет квадратом. Это свойство может использоваться для крапления карт (например, для тузов выбирается числовое представление – квадрат, для других карт – не квадрат).

Список литературы

1. Ниссенбаум О.В. Криптографические протоколы: Учебное пособие. – Тюмень.: ТюмГУ, 2007. – 139 с.

2. Википедия – свободная электронная энциклопедия [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/ (дата обращения: 29.05.2016).