Ментальный покер

Задача: раздать правильную честную игру в интернете

Минимизируем число игроков – 2 и карт – 3

Алиса, Боб, карты $\underset{00}{\alpha}, \underset{01}{\beta}, \underset{10}{\gamma}$, простое число P

Раздать: 1 Карту Алисе (только она должна знать)
2. Карту Бобу (-//-)
3. Одна должна остаться в прикупе)

Вероятность получения всех карт должна быть равномерной

А: (1) $c_A d_A = 1 \bmod (P-1)$ c выбирается случайно,
Б: (2) $c_B d_B = 1 \bmod (P-1)$ d ищется с помощью обобщ. алг. Евкл.

$r_1, r_2, r_3 \in \{1, .., P-1\}$, каждый раз выбираются новые

$R_1 = <r_1 00>$ $R_2 = <r_2 01>$ $R_3 = <r_3 10>$

1. Алиса считает все $x_i = R_i^{c_A} \bmod P$, $i = 1,2,3$ и высылает все их Бобу перемешав в случайном порядке
2. Боб выбирает один x случайно и отправляет Алисе (напр. x_2)
3. Алиса получила карту 01 (β)
4. Боб вычисляет для оставшихся x_i $y_i = x_i^{c_B} \bmod P$ $i = \{1,3\}$ и перемешав, отправляет Алисе
5. Алиса выбирает один y, считает $z = y^{d_A} \bmod P$ и высылает Бобу
6. Боб вычисляет $w = z^{d_B} \bmod P$ и получает R_i

Пример

$P = 23 \qquad c_A = 3 \qquad d_A = 15 \qquad r_1 = 01 \qquad R_1 = 0100$

$c_B = 5 \qquad d_B = 9 \qquad r_2 = 11 \qquad R_2 = 1101$

$r_3 = 10 \qquad R_3 = 1010$

$x_1 = R_1^{c_A} \bmod P = 4^3 \bmod 23 = 64 \bmod 23 = 18$

$x_2 = 12$

$x_3 = 11$

Боб выбрал x_1 – Алисе досталась карта α

$y_1 = x_2^{c_B} \bmod P = 12^5 \bmod 23 = 18$

$y_2 = x_3^{c_B} \bmod P = 11^5 \bmod 23 = 5$

Алиса выбирает y_2, $z = y_2^{d_A} \bmod P = 19$

Боб получает z и вычисляет $w = z^{d_B} \bmod P = 10 = 1010 = R_3$