Задание выполнил Улитин Иван Владимирович, 531 группа

Мысленный покер с тремя игроками

1. Вводится длина простого числа в битах, которое будет общим модулем p и понадобится для генерации пары ключей для каждого из игроков. Затем вводится количество игроков и поочередно имя каждого из игроков. Для каждого из них генерируется пара ключей и сохраняется вместе с общим модулем в отдельный файл для игрока в формате (x, y, p), где x, y - ключи, а p - модуль.
2. Из списка игроков выбирается диллер, который генерирует 52 сообщения (колоду карт). В данном случае колода это файлы, имена которых являются номерами от 0 до 51, при этом содержание их есть перемешанная колода при каждой новой генерации колоды. В каждое сообщение включено случайное число для того, чтобы на последующих этапах протокола диллер мог проверять подлинность сообщений. Диллер зашифровывает все сообщения с помощью своего открытого ключа x.
3. Чтобы диллер по именам файлов не мог отследить карты, осуществляется перемешивание имен файлов. С этого момента перемешивание колоды окончено, и имена файлов не перемешиваются до конца игры.
4. Теперь каждый игрок может отобрать введенное количество произвольных карт из колоды и зашифровать их своим открытым ключом x.
5. Диллер, который не может прочесть чьи-либо сообщения, может расшифровывать их своим закрытым ключом y.
6. Игроки могут расшифровывать сообщения с помощью своих ключей y, чтобы узнать, какие карты им достались.
7. Диллер также может расшифровывать сообщения, чтобы узнать свои карты (если он отдельно себе их раздал), либо расшифровать все оставшиеся карты (колоду).
8. Если кому-то нужно добрать карты, то это осуществляется аналогично шагу 4.

Генерация ключей

Ключи x, y генерируются следующим образом:

1. Выбирается случайным образом такое x, что:
   - $1 \leq x \leq p - 1$
   - НОД$(x, p - 1) = 1$
2. К нему в соответствие выбирается случайным образом такой y, что:
   - $y \cdot x = 1 \pmod{p - 1}$
3. В результате имеем пару (x, y).

Шифрование и дешифрование

Шифрование сообщения a задано функцией E, где $E(a, x, p) = a^x \pmod{p} = e$.

Дешифрование шифра e сообщения a задано функцией D, где $D(e, y, p) = e^y \pmod{p} = a^{x \cdot y} \pmod{p} = a$.