**Мысленный покер с тремя игроками**

1. Каждый игрок генерирует свою пару ключей (открытый/закрытый), но оба ключа держит в секрете до конца игры.

2. Алиса генерирует 52 сообщения (колоду карт). Например, файлы, имена которых являются номерами от 1 до 52, при этом содержание их должно быть перемешанной колодой при каждой новой генерации колоды. В каждое сообщение необходимо включать уникальную случайную строку с тем, чтобы на последующих этапах протокола Алиса могла проверять их подлинность. Алиса зашифровывает все сообщения с помощью своего открытого ключа и отсылает их Бобу.

3. Боб не может прочитать колоду. Но чтобы и Алиса по именам файлов не могла отследить карты, он перемешивает имена файлов. С этого момента перемешивание колоды окончено, и имена файлов не перемешиваются до конца игры. Теперь Боб произвольно отбирает пять из них, шифрует их своим открытым ключом и отправляет Алисе.

4. Боб отсылает остальные 47 сообщений Кэрол.

5. Кэрол, которая не может прочесть ни одного сообщения, произвольно отбирает пять из них, шифрует их своим открытым ключом и отправляет Алисе.

6. Алиса, которая не может прочесть ни одного из полученных сообщений, расшифровывает их своим закрытым ключом и отсылает обратно Бобу или Кэрол, в зависимости от того, от кого она их получила.

7. Боб и Кэрол расшифровывают сообщения с помощью своих ключей, чтобы узнать, какие карты им достались.

8. Кэрол произвольно отбирает пять из 42 оставшихся сообщений и отправляет их Алисе.

9. Алиса расшифровывает сообщения, чтобы узнать свои карты.

10. Колода осталась у Кэрол. Если кому-то (кроме Алисы) нужно добрать карты, то Кэрол отправляет ему оставшуюся колоду, и он повторяет протокол с Алисой. Если карты нужны Алисе, то тот, у кого в данный момент находится шифрованная колода, отсылает ей произвольно выбранные карты в количестве запроса.

11. По окончании игры Алиса, Боб и Кэрол открывают свои карты и пары ключей с тем, чтобы каждый мог убедиться в отсутствии мошенничества.