Министерство образования и науки Российской Федерации

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

Кафедра теоретических основ компьютерной безопасности и криптографии

**Ментальный покер с тремя игроками**

ОТЧЕТ ПО ДИСЦИПЛИНЕ

«Криптографические протоколы»

Лабораторная работа №1

студентки 5 курса 531 группы

специальности 10.05.01 «Компьютерная безопасность»

факультета компьютерных наук и информационных технологий

Громовой Наталии Викторовны

|  |  |  |
| --- | --- | --- |
| Преподаватель  доцент | \_\_\_\_\_\_\_\_\_\_ | В.Е. Новиков |
|  | подпись, дата |  |

Саратов 2018

**Теоретическая часть**

Протокол, аналогичный протоколу броска монеты с помощью открытых ключей, позволяет Алисе и Бобу играть друг с другом в покер по электронной почте. Алиса вместо создания и шифрования двух сообщений, одного для "орла", а другого - для "решки", создает 52 сообщения *М1*, *М2*, ..., *М52*, по числу карт в колоде. Боб случайным образом выбирает пять из них, шифрует своим открытым ключом и посылает обратно Алисе. Алиса расшифровывает сообщения и посылает их обратно Бобу, который расшифровывает их для определения своей "руки". Затем он случайным образом выбирает еще пять сообщений и, не изменяя их, посылает Алисе. Она расшифровывает их, и эти соответствующие карты становятся ее "рукой". В течение игры эта же процедура применяется для сдачи игрокам дополнительных карт. В конце игры Алиса и Боб раскрывают свои карты и пары ключей, чтобы каждый мог убедиться в отсутствии мошенничества.

Для данного протокола необходимым условиям является применение коммутативного шифра. Таким шифром может стать шифр Полига-Хеллмана ­­— он представляет собой несимметричный алгоритм, поскольку используются различные ключи для шифрования и расшифрования. В то же время эту схему нельзя отнести к классу криптосистем с открытым ключом, так как ключи шифрования и расшифрования легко выводятся один из другого. Оба ключа (шифрования и расшифрования) нужно держать в секрете.

Аналогично схеме RSA криптограмма С и открытый текст Р определяются из соотношений:

С = Рe mod n,

Р = Сd mod n.

*Описание:*

Для построения предлагаемой схемы необходимы следующие обозначения: *E* – коммутативный алгоритм шифрования, *D* ­ – соответствующий алгоритм расшифрования; каждому из игроков известно большое простое число *р* и каждый формирует свою пару чисел *e* и *d* таких, взаимно простых с *р-1,* таких что .

Шаг 1. Алиса, Боб и и Кэрол создают пары открытый ключ/закрытый ключ – (*eA*, *dA*), (*eB*, *dB*) и (*eC*, *dC*) соответственно.

Шаг 2. Алиса создает 52 сообщения, по одному для каждой карты колоды. Эти сообщения должны включать некоторую уникальную случайную строку, чтобы Алиса могла проверить их подлинность на последующих этапах протокола. Алиса шифрует все сообщения своим открытым ключом и посылает их Бобу в произвольном порядке.

Еа(М)

Шаг 3. Боб, который не может прочитать не одно сообщение, случайным образом выбирает пять из них. Он шифрует их своим открытым ключом и посылает обратно Алисе.

Ев(ЕА(Мп))

Шаг 4. Боб отправляет Кэрол оставшиеся 47 сообщений.

ЕА(Мп)

Шаг 5. Кэрол, которая не может прочитать не одно сообщение, случайным образом выбирает пять из них. Она шифрует их своим открытым ключом и посылает Алисе.

ЕС(ЕА(М„))

Шаг 6. Алиса, которая не может прочитать ни одно из полученных сообщений, расшифровывает их своим закрытым ключом и посылает обратно Бобу или Кэрол (в соответствии с тем, от кого она их получила).

DA(EB(EA(Mn)))= EB(Mn)

DA(Ec(EA(Mn)))= ЕС(М„)

Шаг 7. Боб и Кэрол расшифровывают сообщения своими ключами, чтобы узнать свои карты

DB(EB(Mn))

Dc(Ec(Mn))

Шаг 8. Кэрол случайным образом выбирает пять из оставшихся 42 сообщений и посылает Алисе. ЕА(Мп)

Шаг 9. Алиса расшифровывает сообщения, чтобы узнать свои карты. DA(EA(Mn))

Шаг 10. В конце игры Алиса, Боб и Кэрол раскрывают свои карты и пары ключей, чтобы каждый мог убедиться в отсутствии мошенничества.

Протокол:

Шаг 1. Генерация ключей.

Для *A*,*B* и *C* – соответственно.

Шаг 2. ?

1)

2)

3)

4)

5)

6)

7)

8)

9)