Сундуки и протоколы: криптография без формул

А. В. Устинов

Шифрование — это всегда интересно. Но и другие разделы современной криптографии могут служить источниками занимательных и исследовательских задач (см. [1, 2]). В докладе планируется обсудить несколько задач, которые позволяют познакомиться с теорией протоколов, используя простой язык «сундуков» и «замков».

Задача 1. $A+B=\heartsuit$**.** Алиса и Боб познакомились друг с другом в дебрях всемирной паутины и подружились. Они беспрепятственно могут переписываться по электронной почте, но им не повезло: они живут в стране Заядлых Коллекционеров. Любая вещь, посланная по почте в обычном ящике, бесследно исчезает. Для решения этой проблемы почтовая индустрия изготавливает прочные сундуки, которые гарантируют безопасную пересылку при условии, что они закрыты на навесной замок. Сундуки бывают любых размеров и на них можно вешать разное количество замков. Замки тоже изготавливаются отменного качества, покупая замок вы имеете гарантии, что ключи от него есть только у вас.

Боб решил послать Алисе в подарок на день рожденья уникальную старинную монету. Как он может это сделать пользуясь услугами почты?

Решение задачи 1 назовем протоколом *безопасной пересылки*.

Задача 2. Предположим, что в стране Коллекционеров есть Спецслужба, которая может контролировать электронные сообщения и пересылку сундуков по почте. Какие слабые места тогда появляются в протоколе безопасной пересылки?

Задача 3. Допустим, что подаренная Бобом монета все-таки была получена Алисой. Как в будущем они могут обезопасить свою корреспонденцию от постороннего вмешательства?

В криптографии подлинность сообщения удостоверяется с помощью протокола *электронной подписи*.

Задача 4. Орел или решка? Алиса и Боб решили кинуть жребий, чтобы определить кто к кому первым приедет в гости. Алиса подбрасывает монету, а Боб пытается угадать, что на ней выпало. Как пользуясь услугами почты они могут обеспечить себе честную игру?

В криптографии аналогичный протокол называется *подбрасывание монеты по телефону*.

Задача 5. Покер по телефону. После состоявшегося знакомства Алиса и Боб (снова находясь в разных городах) захотели сыграть в более азартную игру — упрощенный покер. Его правила таковы. Имеется колода из 10 карт, на которых написаны числа от 1 до 10. Каждый игрок должен получить одну случайную карту, потом делаются ставки, игроки вскрываются, и банк достается игроку имеющему большее число. Как должны действовать Алиса и Боб, чтобы честно поиграть друг с другом в покер, не прибегая к посторонней помощи?

6. Расследование по телефону. Два шерифа соседних городов составили список из восьми лиц, подозреваемых в качестве серийного убийцы. Затем каждый из них

благодаря оперативно-розыскным действиям сумел сократить этот список всего до двух кандидатур. Известно, что сокращенные списки шерифов пересекаются ровно по одному подозреваемому, поэтому если им удастся как-то обменяться информацией, то они совместно смогут арестовать убийцу. Арестовать его в одиночку шерифы не могут. К сожалению, единственным доступным способом что-то сообщить коллеге является совместное выступление по телевизору, которое будут слышать все жители двух городов. Если жители из разговора шерифов смогут понять, кто убийца, то они линчуют его, не дожидаясь его ареста (полный список подозреваемых жителям известен). Помогите шерифам так обменяться информацией, чтобы убийца был именно арестован, а не линчеван жителями.

7. Суперкомпьютеры. В одном НИИ жили четыре суперкомпьютера, попарно соединенные друг с другом в сеть. Днем они решали задачи, которые им навязывали люди, а ночью — развлекались. Сначала они пробовали играть в шахматы, но эта игра им быстро наскучила, поскольку они перебрали все варианты. Потом суперкомпьютеры захотели поиграть друг с другом в карты.

Как должны действовать компьютеры, чтобы честно раздать между собой виртуальную колоду для игры в бридж (раздаются 52 карты по 13 штук каждому)? При этом должны соблюдаться естественные условия, соответствующие честной раздаче реальных карт (все расклады равновероятны, и ни один из игроков не имеет информации о картах других игроков).

Дополнительные условия: 1) компьютеры «честные», т.е. никто из них не нарушает выбранный протокол; в частности, ни один из компьютеров не пытается «сговориться» с другими против кого-либо. 2) компьютеры ничего не забывают; 3) каждый из компьютеров может решить сколь угодно сложную математическую задачу (иначе говоря, понятие «криптографической стойкости» для них абсолютно, а не условно зависит от ложности какой-либо задачи).

Список литературы

[1] Дориченко С. А., Ященко В. В. 25 этюдов о шифрах М.: ТЕИС, 1994.

[2] Зубов А., Зязин А., Овчинников В., Рамоданов Ц. Олимпиады по криптографии и математике для школьников. МЦНМО, Москва, 2006