Решение некоторых задач из курса "Современные задачи криптографии".

Ю. Лифшиц *

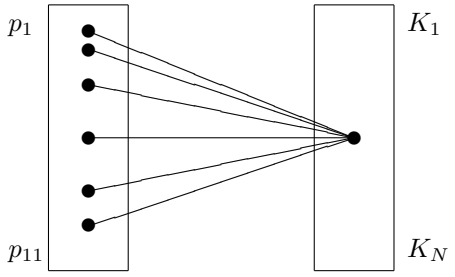
29 ноября 2005 г.

Задача 1 ***(лекция 1):***

Вы хотите повесить несколько обычных замков и раздать ключи, чтобы было выполнено правило доступа "6 из 11". Найти минимальное число замков в этом случае.

Решение *(Дмитрий Ширяев)*:

Итак, от нас требуется найти минимальное число замков, при котором любые шесть из одиннадцати человек смогут открыть любой из них. При этом для пяти или менее человек найдется замок, для которого не будет ключа ни у кого из них. Будем строить двудольный граф. В одной его половине разместим 11 вершин $p_1 \dots p_{11}$, каждая из которых соответствует одному человеку. В другой половине разместим вершины $K_1 \dots K_N$, соответствующие N замкам. Ребро (p_i, K_j) в нашем графе обозначает факт наличия у человека p_i ключа от замка K_j.



Так чему же все-таки равно N? Покажем, что $N = C_{11}^6$. Для доказательства этого факта построим биекцию между множеством ключей и всеми множествами по шесть из одиннадцати человек. В терминах нашего графа это означает следующее. Из любой вершины в правой его половине выходит

*Законспектировал И. Сергей.

6 ребер, которые входят в некое множество из 6 вершин в левой половине. Причем для некоторых K_i и K_j эти множества совпадают, только при $i = j$. Теперь становится понятно, что, какой бы мы замок ни взяли, у кого-то из любых шести человек всегда найдется от него ключ (иначе это противоречило бы построению нашего графа).

Пусть теперь пятеро (или менее) человек вознамерились открыть все замки. Покажем, что для них всегда найдется замок, который они не смогут открыть. Это будет тот замок, ключом от которого располагают шестеро из оставшихся людей. Такой замок существует по построению. Минимальность следует из того, что при меньшем числе ключей для некоторой пятерки человек такого "невскрываемого" замка могло бы и не найтись.

Задача 2 ***(лекция 2):***
Придумать протокол для игры в покер втроем по телефону.

Решение *(Николай Гравин)*:

Алиса, Боб и Карл решили сыграть в покер по телефону. Для определенности будем считать, что никакие двое игроков не находятся в сговоре (иначе игра теряет смысл). Решение представляется весьма простым. Для начала Алиса и Боб генерируют p_A и p_B - некоторые перестановки для 52 карт соответственно, после чего посылают эти перестановки Карлу. Карл использует перестановку $p_A \circ p_B$ на упорядоченное (как именно - оговорено заранее) множество карт, после чего выбирает себе первые 5 из получившейся последовательности. После этого для каждой из оставшихся 47 карт $c_1 \dots c_{47}$ (можно считать их числами из множества $1 \dots 52$) Карл выбирает представление в виде чисел a_i и b_i, таких, что $c_i \equiv a_i + b_i \ mod\ 52$. Затем Карл отслыает Алисе набор $(a_1, \dots, a_{47})$, а Бобу - набор $(b_1, \dots, b_{47})$. После этого Алиса и Боб договариваются о том, что каждый из них выбирает для себя набор карт $(i_1, \dots, i_5)$ и $(j_1, \dots, j_5)$ таким образом, чтобы $i_k \neq j_l$ при любых k и l. Затем они обениваются наборами $(a_{i_1}, \dots, a_{i_5})$ и $(b_{j_1}, \dots, b_{j_5})$ соответственно и получают возможность узнать свои карты.

Как можно, видеть, построенный таким образом протокол удовлетворяет необходимым трем требованиям:

1. Раздача карт случайна
2. Наборы карт не пересекаются
3. Игроки не знают о том, какие карты у соперников (кроме того, что они отличны от его собственных)

В принципе, Карл может выбрать не первые пять карт из получившейся перестановки, а какие-либо другие, но такой обман раскроется по окончании игры, когда Алиса и Боб захотят проверить его честность, обменявшись своими перестановками.

Задача 3 ***(лекция 5):***
Докажите, что $IP \subseteq PSPACE$

Решение *(Николай Гравин)*:

Итак, пусть $L \in IP$. Вспомним, что по определнию $PSPACE$ язык $L \in PSPACE$, если существует полиномиальный по памяти алгоритм P такой, что $x \in L \Leftrightarrow \exists y : P(x, y) = 1$. Для выяснения этого факта будем искать prover P такой, что для любого V $[P(x), V(x)] = 1$. Выяснение существования такого P и будет алгоритмом, полиномиальным по памяти, т. к. перебирая для разных P всевозможные V, мы должны хранить в памяти лишь результаты предыдущих проверок.

Задача 4 ***(лекция 5):***
Пусть $N = pq$. *Пусть у остатка* x *символ Лежандра равен* 1, *то есть или* $x \equiv y^2 \ mod \ N$, *или* x *- квадратичный невычет и по модулю* p, *и по модулю* q. *Как с нулевым разглашением доказать, что* $x \equiv y^2 \ mod \ N$*?*

Решение *(Алексей Диевский)*:

Рассматриваем $x \in (\mathbb{Z}/\mathbb{Z}_N)^*$, то есть x - обратим в $(\mathbb{Z}/\mathbb{Z}_N)$. Тогда возможно два варианта: либо x - квадратичный невычет по модулю p и по модулю q. Для V предлагается следующий алгоритм. С вероятностью $P = \frac{1}{2}$ V производит одно из двух действий:

1. "0": V выбирает случайное чилсо a, такое, что a является сильным квадратичным невычетом по модулю N, т. е. a - квадратичный невычет по модулю p и по модулю q. Число a посылается P.
2. "1": V посылает P число вида r^2x.

Дальше V ждет, что ему отошлет P. P пытается угадать, что было выбрано - "0"или "1"и отсылает результат V. После чего весь цикл повторяется.

Поясним, что пргоисходит. Если изначально P посылал квадратичный вычет, то по тому, что ему послал назад V он легко определит результат, ибо это будет либо a - сильный невычет, либо r^2x - квадратичный вычет, а P обладает достаточной вычислительной мощностью, чтобы проверить, чем является результат. В противном случае, если P врет, он получит за это сильный невычет, и ему придется гадать, какой же из двух вариантов выбрал V. При повторении алгоритма 1000 раз, вероятность удачи P будет равняться $\frac{1}{2^{1000}}$

Замечание: Тонкости из области теории чисел остаются на совести Юры и докладчика. :)

Задача 7 ***(лекция 8):***
Постройте протокол для передачи данных вслепую "1-из-4".

Решение *(Дмитрий Ширяев)*:

Для начала, разберемся в постановке задачи. Предположим, Алиса владеет четырьмя битами a_1, a_2, a_3, a_4. Боб желает получить бит a_i. При этом, получив бит a_i, Боб ничего не должен знать об остальных битах, а Алиса не должна узнать, какой бит запросил Боб.

Для определенности будем считать $i = 3$. Тогда алгоритм будет выглядеть следующим образом.

1. Алиса задумывает два случайных числа c_1 и c_2 и предлагает Бобу выбрать одно число из $a_1 + c_1$ или $a_2 + c_1$ (при этом Боб знает, какое из них какому биту соответствует). Выбор производится согласно протоколу "1-из-2".

2. Затем Бобу предлагается выбрать еще одно число, но уже из $a_3 + c_2$ или $a_4 + c_2$ (аналогично предыдущему шагу).

3. Наконец, Бобу предлагается выбрать одно из чисел c_1 или c_2, причем указывается, что c_1 соответствует первой паре битов, а c_2 - второй (аналогично первым двум шагам).

4. Так как Боб знает, что бит с нужным ему номером находится во второй паре, он выбирает c_2.

5. Теперь Боб знает c_2, $a_3 + c_2$, и одно из чисел $a_1 + c_1$ или $a_2 + c_1$, а значит благополучно получает a_3.

6. При этом Алиса не знает ничего согласно протоколу "1-из-2".

Задача 8 ***(лекция 9):***
Пусть есть физический источник независимых битов, но вероятности 0 и 1 немного отличаются (неизвестно как). Как получить действительно случайную последовательность?.

Решение *(Юрий Лифшиц)*:

1 и 0 выдаются физическим источником с вероятностями p и q, такими, что $p \neq q$. Рассмотрим цепочку битов, порождаемую нашим физическим источником и скомбинируем все биты по парам. Пару (0,1) считать нулем, а пару (1,0) - единицей. Пары же (0,0) и (1,1) будем игнорировать. Нетрудно заметить, что $P(0,1) = P(1,0)$. Таким образом, мы рассматриваем пространство событий появления (0,1) или (1,0), а эти события равновероятны. Таким образом, получили источник действительно случайной последовательности.

Использованные материалы:

1. Презентации курса, предоставленные Ю. Лифшицем
2. Брюс Шнайер, "Прикладная криптография"
3. Конспекты лекций, предоставленные участниками семинара
4. Бумажный конспект лекции 29.11.2005
5. Текстовый редактор WinEdt 5
6. Adobe Acrobat Version 6.0