Системы шифрования с открытым ключом.

Различные задачи по криптографии.

Занятие 3 (лекция)

§ 1. Основная часть

Виды систем шифрования

Системы шифрования

с секретным ключом *с открытым ключом*

Системы шифрования, существующие на данный момент, можно разделить на два класса: *системы с секретным ключом* (системы симметричного шифрования) и *системы с открытым ключом* (системы асимметричного шифрования).

Системы шифрования с секретным ключом

До 1978 года были известны лишь *шифры с секретным ключом*. Так называются шифры, для которых *расшифрование* определяется тем же ключом, что и *зашифрование*. Поэтому ключ нужно хранить в секрете от посторонних. В связи с симметричностью ситуации при использовании секретного ключа используют термин *симметричное шифрование*.

Примером шифра с секретным ключом является *шифр простой замены* типа «пляшущих человечков». Ключом такого шифра служит таблица замены знаков алфавита «человечками». Обозначим через $E_k(u) = v$ результат зашифрования сообщения u на ключе k, а через $D_k(v)$ результат расшифрования v на ключе k. Преобразования, осуществляемые при зашифровании и расшифровании, должны быть такими, чтобы для любых u и k выполнялось соотношение $D_k(E_k(u)) = u$.

Отметим:

1. Расшифрование определяется **тем же** ключом, что и зашифрование.
2. Ключ k держится абонентами *строго в секрете*.

Системы шифрования с открытым ключом

В 1978 году появился первый *шифр с открытым ключом* под названием RSA (образованным первыми буквами разработчиков). Для зашифрования и расшифрования RSA использует *разные ключи* (и, соответственно, разные преобразования). При этом ключ зашифрования объявляется открытым. Более того, нужно чтобы этот ключ записывался в общедоступном справочнике вместе с именем пользователя и другими данными. *Секретным* является ключ расшифрования, причём принадлежать он должен лишь одному пользователю. В связи с асимметричностью ситуации при использовании ключей появился термин *асимметричное шифрование*.

Обозначим через E_A (открытый) алгоритм зашифрования пользователя A, а через D_A – его (секретный) алгоритм расшифрования. Пусть $v = E_A(u)$ – результат зашифрования сообщения u, а $u = D_A(v)$ – результат расшифрования сообщения v. Преобразования должны быть такими, чтобы для любого u выполнялось равенство $D_A(E_A(u))=u$.

Отметим:

1. Расшифрование и зашифрование определяются **разными** ключами пользователя;
2. Ключ зашифрования является *общедоступным*, а ключ расшифрования *держится в секрете.*

Можно привести следующую аналогию асимметричного шифрования. Если отправитель желает передать секретное сообщение, он информирует об этом получателя (например, телефонным звонком). Получатель присылает по почте почтовый ящик с прорезью с закрытым замком. Отправитель опускает в прорезь свое сообщение (тем самым, “шифрует” его) и отсылает ящик по почте получателю. Получатель вынимает сообщение (производит “расшифрование”), воспользовавшись своим ключом. Злоумышленнику, которому отправленный ящик попадает в руки, практически невозможно изъять из него сообщение через прорезь. В такой системе шифрования

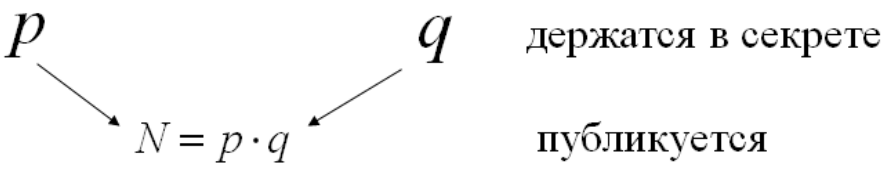
прямое и обратное преобразования информации имеют различный характер. “Открытый ключ” − это, по сути дела, − прорезь, “секретный ключ“ − это ключ от замка почтового ящика. Знание открытого ключа не позволяет определить секретный ключ.

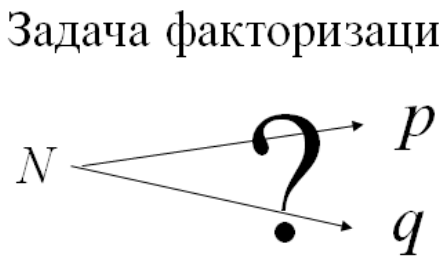
Немного об RSA

Сейчас известно достаточно много различных асимметричных криптосистем. Стойкость таких систем основывается одной из сложных математических проблем. Одной из таких проблем является задача разложения числа N на простые множители, такая задача носит название *задачи факторизации* (англ. factor - множитель). В частности данная задача представляет интерес, когда N является произведением двух простых чисел. Понятно, что если N небольшое, то решить эту задачу не так сложно. Можно перебирать последовательно все простые числа, меньшие N, и пытаться нацело делить N на перебираемое простое число. Но если же N большое, то в общем случае данная задача является весьма сложной.

Одной из самых известных криптосистем с открытым ключом в основе построения которой лежит задача разложения большого числа на большие множители является система RSA (от имен своих разработчиков: Rivest, Shamir, Adleman).

Суть системы заключается в следующем. Выбираются большие простые числа p и q, которые держаться в секрете. Публикуется их произведение $N=pq$, а также выработанный определенным образом ключ зашифрования. Ключ расшифрования держится в секрете и вырабатывается так же определенным образом, **используя знание** *факторизации* числа N (то есть знание p и q). Далее, любой желающий отправить, скажем нам, сообщение зашифрует его на нашем открытом ключе зашифрования и отправит нам криптограмму. При этом любой, отличный от нас пользователь, который перехватит криптограмму не сможет ее расшифровать, так как он не сможет выработать ключ расшифрования, поскольку не знает факторизации N.





§ 2. Решение задач

Уже говорилось, что если N небольшое, то решить задачу факторизации не так сложно. Можно перебирать последовательно все простые числа, меньшие N, и пытаться нацело делить N на перебираемое простое число. Такой способ известен как *метод пробных делений*.

А если N содержит сотни разрядов в своей записи? В этом случае применение метода пробных делений является очень трудоемким. Однако, если известно, что $N=p\cdot q$, где p и q - близкие простые числа (то есть их разность - число небольшое), то разложить большое N на простые множители можно использовав *метод Ферма*. В основе этого метода лежит тот факт, что в этом случае существует z такое, что:

$$p = z - t,$$
$$q = z + t.$$

а z – небольшое.

Задача № 1

Число $N = 99873791$ является произведением двух простых чисел p и q, причем $p - q \leq 500$. Разложить это число на простые множители.

Решение:

Пусть $p = z - t$, а $q = z + t$. Тогда

$$N = p \cdot q = (z - t)(z + t) = z^2 - t^2,$$

$$z^2 = N + t^2,$$

$$z = \overline{N + t^2},$$

$$z > \overline{N}.$$

Причем отметим, в силу того, что p и q - близкие простые числа, $p - q \leq 500$, то значение z близко к значению $\overline{N}$, но немного его превосходит. Будем проводить подбор значения для этого числа. В данном случае, нетрудно подсчитать (на калькуляторе, или заметив, что 9990< $\overline{N}$<10000), что целая часть корня $\overline{N}$ - это 9993. Тогда первое возможное значение для z - 9994.

1. Пусть $z = 9994$. Тогда $t^2 = z^2 - N = 99880036 - 99873791 = 6245$, но значение $\overline{6245}$ - число не целое.
2. Пусть $z = 9995$. Тогда $t^2 = z^2 - N = 99900025 - 99873791 = 26234$, но значение $\overline{26234}$ - тоже не целое.
3. Пусть $z = 9996$. Тогда $t^2 = z^2 - N = 99920016 - 99873791 = 46225$ и $t = \overline{46225} = 215$

Подставив полученные значения для z и t, получаем, что $p = 9996 - 215 = 9781$, $q = 9996 + 215 = 10211$.

Ответ: 99873791=9781·10211.

Задача № 2

Сколько имеется натуральных чисел, меньших $N = p \cdot q$ и взаимно простых с N, где p и q – различные простые числа?

Решение:

Сначала заметим, что если $N = pq$, где p и q – простые числа, то количество натуральных чисел, меньших N и взаимно простых с N равно $(p-1)(q-1)$ (обозначим это число $\varphi(N)$). Действительно, всего имеется $pq-1$_натуральных чисел, меньших N. Из них не взаимнопросты с N те числа, которые делятся либо на p, а именно $p, 2p, \ldots, (q-1)p$ (всего $(q-1)$ чисел), либо на q, это числа $q, 2q, \ldots, (p-1)q$ (всего $(p-1)$ чисел). Значит

$$\varphi(N) = pq - 1 - (p-1) - (q-1) = pq - p - q + 1 = (p-1)(q-1).$$

Ответ: $(p-1)(q-1)$.

Задача № 3

Известно, что число $N = 203060593$ является произведением двух простых чисел p и q, а количество натуральных чисел, меньших и взаимно простых с N, равно 203030388. Найдите числа p и q.

Решение:

Воспользуемся предыдущей задачей. Пусть так же $\varphi(N)$ – количество натуральных чисел, меньших N и взаимнопростых с ним. Тогда $\varphi(N) = (p-1)(q-1)$. Получим следующую систему уравнений с двумя неизвестными.

$$\begin{cases} pq = N \\ (p-1)(q-1) = \varphi(N) \end{cases}$$

Раскроем скобки во втором уравнении и подставим в него первое уравнение. Получим следующую равносильную систему.

$$\begin{cases} pq = N \\ p + q = N + 1 - \varphi(N) \end{cases}.$$

В силу теоремы обратной теореме Виета, числа p и q являются решением квадратного уравнения.

$$x^2 - (N + 1 - \varphi(N))x + N = 0$$

$$x^2 - 30206x + 203060593 = 0$$

Решим его, для этого посчитаем дискриминант.

$$\sqrt{D} = \sqrt{100160064}$$

Чтобы извлечь корень из дискриминанта можно подбирать возможные значение и возводить их в квадрат.

$$10002,\ 10008,\ 10012,\ 10018\ldots$$

$$10008^2 = 100160064$$

Итак:

$$x_1 = \frac{30206 - 10008}{2} = 10099 = p$$

$$x_2 = \frac{30206 + 10008}{2} = 20107 = q$$

Ответ: 10099, 20107.

Задача № 4

Пусть $N = 713$ является произведением двух простых чисел p и q. Найти эти числа.

Решение:

Поскольку N является сравнительно малым числом, то для его факторизации можно воспользоваться методом пробных делений.

Будем последовательно рассматривать все простые числа, меньшие N и делить число N на эти числа. Если после деления число получается целым - то задача решена. Иначе переходим к другому простому числу. Проверку начнем с простого числа p=3. Получающиеся данные занесем в таблицу.

p=	3	5	7	11	13	17	19	23
N/p=	237,6...	142,6	101,8...	64,8...	54,8...	41,9...	37,5...	31

Из приведенной таблицы видно, что при p=23 происходит деление нацело числа N: $N = 713 = 23 \cdot 31$ и q=31.

Ответ: 23, 31.

Задача № 5

Для открытия подземелья в волшебной стране надо правильно назвать три целых числа a,b,c, служащих коэффициентами квадратичной функции $f(x) = ax^2 + bx + c$. Представителям четырёх рас были переданы следующие значения функции: троллям – значение $f(21)$, эльфам – $f(24)$, гномам – $f(25)$, оркам – $f(28)$. Когда представители рас встретились, чтобы совместно найти a,b,c и открыть подземелье, один из представителей, чтобы

сорвать мероприятие, предъявил неверное значение. Выясните, кто это был, если известно, что тролли предъявили число 273, эльфы – 357, гномы – 391, орки – 497.

Решение:

Докажем тот факт, что разность значений квадратичной функции должна делиться на разность значений аргументов.

Пусть $u \neq v$ и $f(x) = ax^2 + bx + c$. Рассмотрим разность:

$$f(u) - f(v) = au^2 + bu + c - (av^2 + bv + c) = a(u^2 - v^2) + b(u - v)$$
$$= (u - v)\ a(u + v) + b\ .$$

Из данного равенства видно, что $f(u) - f(v)$ делится на $u - v$.

Проверим выполнение этого факта для различных пар значений:

- для первого и второго: 357–273=84 делится на 3;
- для третьего и четвертого: 497–391=106 не делится на 3; следовательно, значение исказили или гномы, или орки;
- для первого и третьего: 391–273=118 не делится на 4, следовательно, значение исказили тролли или гномы.
- для второго и четвертого: 497–357=140 делится на 4.

Таким образом, исказить значение могли только гномы.

Ответ: гномы сообщили неверное значение.

Задача № 6

Для зашифрования натурального числа m используется граф, представляющий собой множество вершин, некоторые из которых соединены друг с другом прямой линией. Вершины графа, соединенные друг с другом, называют *соседними*. Зашифрование состоит в выполнении следующих действий. В вершины графа записываются натуральные числа так, чтобы их сумма была равна m. Затем к числу в каждой вершине прибавляются числа в соседних вершинах. В результате получается граф, в котором «зашифровано» число m. Пример: для зашифрования числа 8 будем использовать граф на рис. 1. В его вершины поместим числа, сумма которых равна 8 (рис. 2). Затем к каждому числу прибавим числа в соседних вершинах. Результат

зашифрования указан на рис. 3. На рис. 4 приведен результат зашифрования некоторого числа. Найдите его.

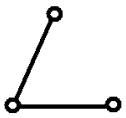


Рис. 1

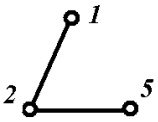


Рис. 2

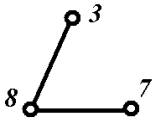


Рис. 3

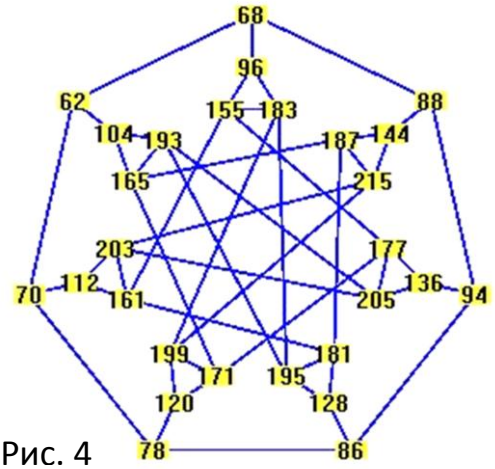


Рис. 4

Решение:

Граф, используемый в задаче, обладает следующим свойством: из множества всех его вершин можно выделить такое подмножество V (отмеченное на рис. 5 кружочками), что любая вершина графа лежит в окрестности ровно одной вершины из V. Окрестностью вершины графа называют множество соседних с ней вершин, включая её саму. Очевидно, что искомое число равно сумме чисел, расположенных в вершинах из множества V: 112+104+96+144+136+128+120=840.

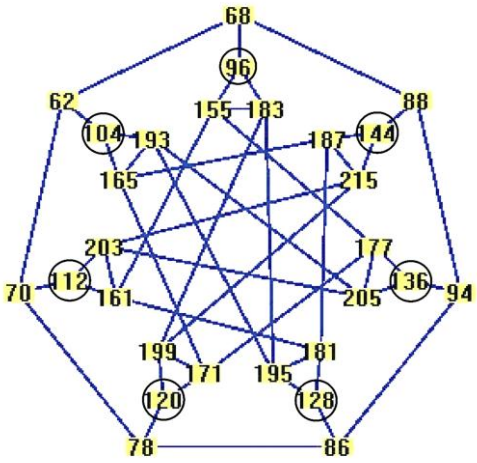


Рис. 5

Ответ: 840.

Задача № 7

Известно, что три числа a_1, a_2, a_3 были получены следующим образом. Сначала выбрали натуральное число A и нашли числа $A_1 = A_{16}, A_2 = A/2_{16}, A_3 = A/4_{16}$, где X_{16} – остаток от деления целой

части числа X на 16 (например, $[53/2]_{16}=10$). Затем было выбрано целое число B такое, что $0\le B\le 15$. Числа A_1, A_2, A_3 и B записывают в двоичной системе счисления, т.е. представляют каждое из них в виде цепочки из 0 и 1 длины 4, приписывая слева необходимое число нулей. Такие цепочки условимся складывать посимвольно «в столбик» без переносов в следующий разряд_согласно правилу: $1+1=0+0=0$ и $0+1=1+0=1$, а саму операцию посимвольного сложения обозначим символом $\oplus$. Например, $3\oplus 14=(0011)\oplus(1110)=(1101)=13$. Положим $a_1=A_1\oplus B$, $a_2=A_2\oplus B$, $a_3=A_3\oplus B$. Найдите все возможные значения числа a_3, если известно, что $a_1=10, a_2=4$.

Решение:

Пусть в двоичной системе счисления $A=(x_n,...,x_0)$. Тогда $A_1=(x_3,x_2,x_1,x_0)$, $A_2=(x_4,x_3,x_2,x_1)$, $A_3=(x_5,x_4,x_3,x_2)$. Следовательно,

$$a_1\oplus a_2 = A_1\oplus B \oplus A_2\oplus B = A_1\oplus A_2=(x_3\oplus x_4, x_2\oplus x_3, x_1\oplus x_2, x_0\oplus x_1),$$

$$a_3\oplus a_2 = A_3\oplus B \oplus A_2\oplus B = A_3\oplus A_2=(x_5\oplus x_4, x_4\oplus x_3, x_3\oplus x_2, x_2\oplus x_1).$$

Итак, если вычислить $a_1\oplus a_2$, то три младших бита $a_3\oplus a_2$ будут найдены, а старший бит будет произвольным.

Вычислим значение $a_1\oplus a_2$:

$$\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ \hline 1 & 1 & 1 & 0 \end{array}.$$

Тогда возможные значения $a_2\oplus a_3$ имеют вид *,1,1,1 , и $a_3=a_2\oplus(a_3\oplus a_2)$:

$$\begin{array}{cccc} 0 & 1 & 0 & 0 \\ * & 1 & 1 & 1 \\ \hline * & 0 & 1 & 1 \end{array}$$

Итак, $a_3=11$, либо $a_3=3$. Можно убедиться в том, что оба варианты верны, если рассмотреть последовательности с параметрами A=11, либо A=43 и B=1.

Ответ: 11 и 3.

Задача № 8

Для прохода в учреждение необходимо предъявить пятизначную комбинацию, состоящую из нулей и единиц. Устройство распознавания представляет собой упрощённую модель нейрона – клетки головного мозга (см. рис. 6).

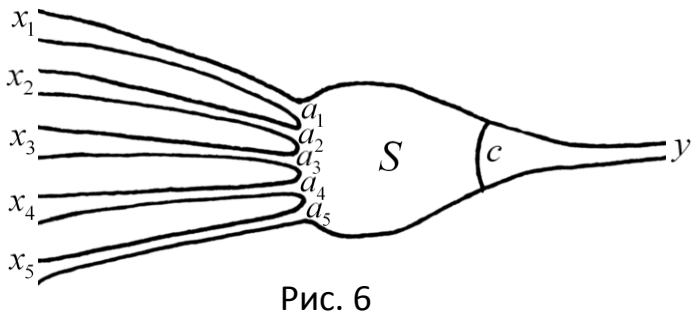


Рис. 6

Пятизначная комбинация x_1, x_2, x_3, x_4, x_5 по пяти каналам поступает в клетку, где её компоненты умножаются на фиксированные целые числа a_1, a_2, a_3, a_4, a_5, и вычисляется сумма $S = a_1x_1 + a_2x_2 + a_3x_3 + a_4x_4 + a_5x_5$. Проход в учреждение открывается, только если $S \geq c$, где $c-$ некоторое фиксированное целое число. В табл. 1 представлены те комбинации, при предъявлении которых проход открывается, а в табл. 2 – для которых проход закрыт.

Таблица 1

1,0,1,1,0	1,1,0,1,0	1,1,1,1,1

Таблица 2

1,0,1,0,0	0,0,1,1,0	1,1,0,1,1	1,0,1,1,1

Найдите ещё одну комбинацию, открывающую проход в учреждение.

Решение:

Для комбинации 1,0,1,1,0 – проход открыт, а для 0,0,1,1,0 – проход закрыт. То есть при изменении значения первой координаты с 1 на 0 значение суммы становится меньше c, поэтому очевидно, что $a_1 > 0$. Аналогично:

$$\left.\begin{array}{l}1,1,1,1,1 \text{ - открыто}\\ 1,0,1,1,1 \text{ - закрыто}\end{array}\right\} \Rightarrow a_2 > 0;$$

$$\left.\begin{array}{l}1,1,1,1,1 \text{ - открыто}\\ 1,1,0,1,1 \text{ - закрыто}\end{array}\right\} \Rightarrow a_3 > 0;$$

$$\left.\begin{array}{l}1,0,1,1,0 \text{ - открыто}\\ 1,0,1,0,0 \text{ - закрыто}\end{array}\right\} \Rightarrow a_4 > 0;$$

$$\left.\begin{array}{l}1,0,1,1,0 \text{ - открыто}\\ 1,0,1,1,1 \text{ - закрыто}\end{array}\right\} \Rightarrow a_5 < 0.$$

Поэтому заведомо пройдет комбинация, максимизирующая значение суммы S, а именно 1,1,1,1,0. Отметим, что задача составлена таким образом, что других решений нет.

Ответ: 1,1,1,1,0.