КРИПТОГРАФИЯ

Авторы: А. М. Зубков

КРИПТОГРАФИЯ (от *крипто*... и ...*графия*), 1) наука о методах преобразования информации для её защиты при передаче по незащищённым каналам связи и о способах практич. реализации этих методов.

Правило криптографич. преобразования информации называется шифром, процесс этого преобразования – зашифрованием, процесс преобразования зашифрованного сообщения в исходное – расшифрованием. Термин «дешифрование» обозначает процесс восстановления исходного сообщения по зашифрованному, который осуществляется посторонним лицом, не имеющим в начале этого процесса полного знания о способе расшифрования. В классич. схеме шифр состоит из двух осн. элементов: секретного ключа (который не должен быть известен никому, кроме отправителя и получателя сообщения) и способа преобразования пары (сообщение, ключ) в зашифрованное сообщение и пары (зашифрованное сообщение, ключ) – в исходное сообщение.

Первые упоминания о К. встречаются в рукописных источниках Древней Индии и Древней Греции. Голл. криптограф О. Керкгоффс в 1883 сформулировал правило, согласно которому стойкость (надёжность) шифра должна обеспечиваться единственным условием: секретный ключ не известен посторонним. Иными словами, шифр должен быть таким, чтобы даже при полностью известных правилах зашифрования и расшифрования было невозможно, не зная ключа, провести дешифрование сообщения (по крайней мере, за время, в течение которого содержащаяся в сообщении информация должна оставаться секретной).

Криптографич. методы широко используются в разл. системах защиты информации. Для решения задач разработки шифров и методов дешифрования в разное время привлекались мн. учёные, среди которых были математики, напр. Ф. *Виет*,

Х. *Гольдбах*, Н. *Винер*, А. *Тьюринг*. Основы совр. теоретич. К. и теории информации были заложены в годы 2-й мировой войны К. *Шенноном*. Он предложил рассматривать шифр как отображение прямого произведения множества

Z всех потенциально возможных сообщений и множества

K ключей в множество

E зашифрованных текстов; при любом фиксированном ключе это отображение

Z в

E должно быть обратимым. Шеннон доказал, что шифр может быть совершенным (т. е. принципиально не дешифруемым) только в случае, когда число разл. ключей не меньше числа возможных сообщений, и что если это условие выполнено, то можно построить совершенный шифр. Примером совершенного шифра является шифр гаммирования. Если исходное сообщение представлено в виде двоичной последовательности

$m_1, m_2, \ldots, m_T$, состоящей из нулей и единиц, то в качестве ключа нужно случайно и равновероятно выбрать двоичную последовательность

$\gamma_1, \gamma_2, \ldots, \gamma_T$ из множества всех

2^T двоичных последовательностей длины

T; тогда совершенным будет шифр, переводящий$m_1,m_2,…,m_T в

m_1+γ_1,m_2+γ_2,…,m_T+γ_T (все сложения проводятся по модулю 2), и получатель, зная

$\gamma_1, \gamma_2, \ldots, \gamma_T$, может восстановить исходное сообщение, вычислив

$(m_1 + \gamma_1) + \gamma_1 = m_1, (m_2 + \gamma_2) + \gamma_2 = m_2, \ldots, (m_T + \gamma_T) + \gamma_T = m_T$. При этом отправитель и получатель должны заранее согласовать значение ключа

$\gamma_1, \gamma_2, \ldots, \gamma_T$, пользуясь каналом связи, который заведомо защищён от всех посторонних (напр., переслать ключ в запечатанном конверте с надёжным курьером). Если посторонний, у которого нет никакой информации о

$\gamma_1, \gamma_2, \ldots, \gamma_T$, попытается восстановить исходное сообщение, перебирая все возможные варианты последовательности

$\gamma_1, \gamma_2, \ldots, \gamma_T$, то он получит все возможные двоичные последовательности длины

T, в т. ч. и

$m_1, m_2, \ldots, m_T$, но у него не будет оснований выделить сообщение

$m_1, m_2, \ldots, m_T$ из множества всех остальных комбинаций
T двоичных знаков. Неудобство указанного шифра связано с необходимостью использования защищённого канала связи для передачи ключей, суммарная длина которых не меньше суммарной длины будущих секретных сообщений. Поэтому на практике используются шифры, в которых объём ключей существенно меньше объёма передаваемых секретных сообщений. Такие шифры не могут быть совершенными; вообще говоря, зашифрованные с их помощью сообщения можно дешифровывать с помощью полного перебора всех возможных ключей. Под стойкостью шифра обычно понимают время работы наилучшего алгоритма вычисления секретного ключа по известным парам исходных и зашифрованных сообщений и известным правилам зашифрования. Однако существующие методы позволяют получать только верхние оценки стойкости шифров (а именно, оценки времени работы конкретных алгоритмов вычисления ключа).

К. использовалась, как правило, для защиты воен. и гос. секретов, и содержательные сведения о ней засекречивались. В последние десятилетия возник спрос на криптографич. методы защиты информации со стороны коммерч. организаций. Т. к. их потребности и возможности отличаются от потребностей и возможностей государств, появились стимулы быстрого развития новых криптографич. методов с общедоступным обоснованием их надёжности в открытой литературе.

Как правило, информация передаётся по каналам связи в осн. в виде двоичных последовательностей. Ввиду больших объёмов передаваемой секретной информации и сложности криптографич. преобразований они реализуются с помощью спец. электронных устройств (шифраторов) или программ для ЭВМ. Перед началом работы в такой шифратор необходимо ввести короткий (по сравнению с объёмом обрабатываемой информации) секретный ключ, который отправитель и получатель должны согласовать способом, исключающим возможность получения к.-л. информации об этом ключе посторонними.

Совр. шифраторы делятся на 2 класса: поточные и блочные. Поточные шифраторы представляют собой электронные устройства с ячейками памяти и специализир. процессорами; они вырабатывают последовательности некоторых знаков и

используют их вместо случайной равновероятной последовательности в шифре гаммирования. Последовательность, вырабатываемая потоковым шифратором, однозначно определяется ключевыми параметрами, задающими начальные состояния ячеек памяти конечного автомата и выбор тех или иных вариантов работы процессоров. Это позволяет отправителю и получателю, согласовавшим заранее значения ключевых параметров, вырабатывать одну и ту же последовательность $\gamma_1, \gamma_2, \ldots, \gamma_T$. Блочные шифраторы разбивают исходное сообщение, представленное в виде двоичной последовательности, на блоки одинакового размера (напр., по 64, 128 или более битов), вычисляют образы этих блоков при взаимно однозначном отображении, конкретный вид которого зависит от секретного ключа, и объединяют образы блоков в зашифрованное сообщение. Получатель, используя тот же секретный ключ, что и отправитель, разбивает полученное сообщение на блоки и, применяя к ним обратное отображение, восстанавливает исходное сообщение.

Классич. схемы шифрования связаны с предварит. обменом секретными ключами между отправителем и получателем. Такой обмен можно осуществить, если общее число абонентов невелико, но он становится практически неосуществимым, если количество абонентов, желающих связываться друг с другом, исчисляется тысячами. Эти потребности оказались одним из стимулов разработки новых принципов шифрования.

В схеме шифрования с открытым ключом, предложенной в 1976 амер. учёными У. Диффи и М. Хеллманом, используются семейства $\{E_e, e \in M\}$ и $\{D_d, d \in M\}$ отображений зашифрования и расшифрования соответственно, действующие на конечном множестве K (напр., на множестве ключей шифратора) и обладающие следующими свойствами: а) для каждого $e \in M$ существует такое $d \in M$, что E_e и D_d – взаимно обратные отображения; б) задача нахождения значения k из множества

K по отображению

E_e и значению

$z = E_e(k)$ вычислительно неразрешима за заданное время; в) существуют не очень сложные способы вычисления значений отображений

E_e и

D_d и построения пар взаимно обратных отображений

(E_e, D_d).

Если такие семейства выбраны, то любой абонент

A может выработать пару взаимно обратных отображений

(E_e, D_d), сообщить всем желающим правило вычисления отображения

E_e (открытый ключ), а правило вычисления

D_d (секретный ключ) держать в секрете. Любой абонент

B, чтобы передать абоненту

A значение

k в виде, защищённом от посторонних, может передать абоненту

A по общедоступному каналу связи значение

$z = E_e(k)$. Тогда абонент

A, знающий отображение

D_d, сможет восстановить

k по

z, а посторонние, не знающие

D_d и не имеющие возможности построить

D_d по

E_e, не смогут этого сделать. Т. к. математически строго обоснованные примеры отображений, удовлетворяющих условию б), ещё не найдены, У. Диффи и М. Хеллман предложили использовать для построения систем шифрования с открытым ключом алгоритмич. задачи, считающиеся вычислительно сложными. Ныне предложен ряд систем шифрования с открытым ключом, основанных на сложности решения задач типа разложения натуральных чисел на простые множители, вычисления квадратного корня в мультипликативной группе вычетов по составному модулю, дискретного логарифмирования [т. е. решения сравнения вида

$ax \equiv b \pmod{n}$, где

n – достаточно большое натуральное число], аналогичных задач для групп эллиптич. кривых над конечными полями и некоторых других.

Потребности коммерческих и финансовых организаций, а также особенности электронных средств связи, задачи защиты электронных баз данных и т. п. стимулировали разработку ряда новых направлений использования криптографич. методов: защиты информации в компьютерных сетях, т. н. электронной подписи, идентификации пользователя (как при деловой переписке, так и при использовании электронных кредитных карт), методов разделения секрета (таких способов разделения секретной информации между
n лицами, которые не позволяют получить никакой информации о секрете, если одновременно не соберётся хотя бы
k лиц из этой группы) и т. п.

При разработке и изучении шифров широко используются методы и результаты алгебры, теории чисел, дискретной математики, комбинаторики, теории вероятностей, математич. статистики. Потребности К. порождают нетривиальные математич. задачи, что существенно (хотя и не всегда явно) влияет на процесс развития теоретич. математики.

Практически все криптографич. способы преобразования информации являются детерминированными. При анализе способов шифрования часто используются вероятностные методы, применяемые к вероятностным моделям детерминированных криптографич. алгоритмов. В кон. 20 – нач. 21 вв. в К. стали проникать идеи и методы *квантовой теории информации* и *квантовой связи*.

2) Тайнопись, система изменения письма с целью сделать текст непонятным для непосвящённых.

3) Раздел *палеографии*, изучающий графику систем тайнописи.

Литература

Лит.: Шеннон К. Э. Работы по теории информации и кибернетике. М., 1963;Diffie W.,

Hellman M. E. New directions in cryptography // IEEE Transactions on Information Theory. 1976. Vol. 22. P. 644–654; Саломаа А. Криптография с открытым ключом. М., 1996; Menezes A. J., Oorschot P. C. van, Vanstone Scott A. Handbook of applied cryptography. Boca Raton, 1997; Кан Д. Взломщики кодов. М., 2000; Коблиц Н. Курс теории чисел и криптографии. М., 2001; Соболева Т. А. История шифровального дела в России. М., 2002; Шнайер Б. Прикладная криптография. М., 2002; Основы криптографии. 3-е изд. М., 2005.