Шифрование

Один из методов защиты информации от неправомерного до-  
ступа — это шифрование, т. е. кодирование специального вида.

Шифрование — это преобразование (кодирование) открытой  
информации в зашифрованную, недоступную для понимания  
посторонними.

Шифрование применяется в первую очередь для передачи сек-  
ретной информации по незащищённым каналам связи. Шифро-  
вать можно любые данные — тексты, рисунки, звук, базы данных  
и т. д.

Человечество применяет шифрование с того момента, как по-  
явилась секретная информация, которую нужно было скрыть от  
врагов. Первое известное науке шифрованное сообщение — еги-  
петский текст, в котором вместо принятых тогда иероглифов  
были использованы другие знаки.

Методы шифрования и расшифровывания сообщения изучает  
наука криптология, история которой насчитывает около четырех  
тысяч лет. Она состоит из двух ветвей: криптографии и крипто-

анализа.

Криптография — это наука о способах шифрования информации.  
Криптоанализ — это наука о методах и способах вскрытия шифров.

Обычно предполагается, что сам алгоритм шифрования извес-  
тен всем, но неизвестен его ключ, без которого сообщение невоз-  
можно расшифровать. В этом заключается отличие шифрования  
от простого кодирования, при котором для восстановления сооб-  
щения достаточно знать только алгоритм кодирования.

Ключ — это параметр алгоритма шифрования (шифра),  
позволяющий выбрать одно конкретное преобразование из всех  
вариантов, предусмотренных алгоритмом. Знание ключа позволяет  
свободно зашифровывать и расшифровывать сообщения.

Все шифры (системы шифрования) делятся на две группы —  
симметричные и несимметричные (с открытым ключом).

Симметричный шифр означает, что и для шифрования, и для  
расшифровывания сообщений используется один и тот же ключ.  
В системах с открытым ключом используются два ключа — от-  
крытый и закрытый, которые связаны друг с другом с помощью  
некоторых математических зависимостей. Информации шифрует-  
ся с помощью открытого ключа, который доступен всем жела-  
ющим, а расшифровывается с помощью закрытого ключа, извест-  
ного только получателю сообщения.

Криптостойкость шифра — это устойчивость шифра  
к расшифровке без знания ключа.

Стойким считается алгоритм, который для успешного раскры-  
тия требует от противника недостижимых вычислительных ре-  
сурсов. недостижимого объёма перехваченных сообщений или та-  
кого времени, что по его истечении защищённая информация  
будет уже не актуальна.

Шифр Цезаря1 — один из самых известных и самых лревних  
шифров. В этом шифре каждая буква заменяется на другую, рас-  
положенную в алфавите на заданное число позиций к вправо от  
нее. Алфавит замыкается в кольцо, так что последние символы  
заменяются на первые. На рисунке 10.2 — пример шифра Цезаря  
(со сдвигом 3У1.

/,5

я

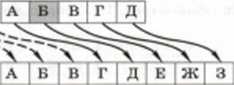


Рис. 10.2

Знаменитая фраза «ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ» при ис-  
пользовании шифра Цезаря со сдвигом 3 будет закодирована так:

ТУЛЫИО ЦКЛЗИОТСДИЗЛО

Если первая буква алфавита имеет код 0, вторая — код 1  
и т. д., алгоритм шифрования может быть выражен формулой

у \*\* (х + k) mod л,

где х — код исходного символа, к — величина сдвига, у — код  
символа-замены, л — количество символов в Алфавите, а запись  
(х \* к) mod п обозначает остаток от деления х +■ к на л. Оперпция  
взятия остатка от деления необходима для того, чтобы замкнуть  
алфавит в кольцо. Например, при использовании русского алфа-  
вита (32 буквы, без буквы «Ё») для буквы «Я» (код 31) получаем  
код заменяющего символа (31 + 3) mod 32 - 2, это буква «В».

Ключом для шифра Цезаря служит сдвиг к, если его знать, то  
сообщение легко расшифровать. Для этого исиользуется формула

\* - (у - \* + л) mod л.

Шифр Цезаря относится к шифрам простой подстановки, так  
как каждый символ исходного сообщения заменяется на другой  
СИМВОЛ из того же алфавита. Такие шифры легко раскрываются с  
помощью частотного Анализа, потому что в каждом языке часто-  
ты встречаемости букв примерно постоянны для любого достаточ-  
но большого текста.

Значительно сложнее сломать шифр Виженерд1, который стал  
естественным развитием шифра Цезаря. Для использования шиф-  
ра Виженера исиользуется ключевое слово, которое задаст пере-  
менную величину сдвига. Например, пусть ключевое слово —  
«ЗАБЕГ». По таблице (рис. 10.3) определяем коды букв.

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |  |
| A | В |  | Г | Д | Е | Ж | з | И | ЙЫ | |

Рис. 10.3

Получаем: «3» — 7, «А» — О, «Б» — 1. «Е» — 5, «Г» — 3.  
Эго значит, что для кодирования первой буквы любого текста ис-  
пользуется сдвиг 7, для кодирования второй — О (символ не ме-  
няется) и т. д. Для пятой буквы используется сдвиг 3, а для шее-

той — снова 7 (начинаем «проходить» кодовое слона с начала).  
Фралп «ПРИШЕЛ УВИДЕЛ ПОБЕДИЛ• при использовании шиф-  
ра Виженера с ключом «ЗАБЕГ, будет закодирована в виде  
«ЦРЙЭИТ УГНЗМЛ РУДМДЙР..

Шифр Виженера обладает значительно более высокой крип-  
тостойкостью, чем шифр Цезаря. Это значит, что его труднее рас-  
крыть — подобрать нужное ключевое слово. Теоретически, если  
длныа ключа равна длине сообщения и каждый ключ использует-  
ся только один раз, шифр Виженера обладает абсолютной крипто-  
стойкостью — взломать его невозможно.

Хэширование и пароли

В современных информационных системах часто используется  
вход по паролю. Вели при этом где-то хранить пароли всех поль-  
зователей, систем» становится очень ненадежной, потому что  
• утечка» паролей позволит сразу получить доступ к данным.  
Вместе с тем кажется, что пароли обязательно где-то нужно хра-  
нить, иначе пользователи не смогут войти в систему. Одняко это  
не совсем так. Можно хранить не пароли, л некоторые числа, полу-  
ченные в результате обработки паролей. Простейший вариант —  
сумма кодов символов, входящих в пароль. Для пароля «А123»  
такая сумма равна

215 - 65 (код «А») + 49 (код «1») + 50 (код »2») + 51 (код »3»).

Фактически мы определили функцию //(АО\* которая сообще-  
ние М любоеI длины превращает в короткий код т. Такую функ-  
цию называются хэш-функцией (от англ. hash — мешанина, кро-  
шить), а само полученное число — хэш-кодом, хэш-суммой или  
просто хэшем исходной строки. Важно, что. зная хэш-код, невоз-  
можно восстановить исходный пароль! В этом смысле хэширова-  
ние — это необратимое шифрование.

Итак, вместо пароля «А123» мы храним число 215. Когда  
пользователь вводит пароль, мы считаем сумму кодов символов  
этого пароля и разрешаем вход в систему только тогда, когда она  
равна 215. И вот здесь возникает проблема: существует очень  
много паролей, для которых паша хэш-функция дает значение  
215, например «В023». Такая ситуация — совпадение хэш-кодов  
различных исходных строк — называется коллизией (англ.  
collision — столкновение). Коллизии будут всегда — ведь мы  
•сжимаем» длинную цепочку байтов до числа. Казалось бы. ниче-  
го хорошего не получилось: если взломщик узнает хэш-код, то,  
зная алгоритм его получения, он сможет легко подобрать пароль с  
таким же хэшем и получить доступ к данным. Однако это прои-  
зошло потому, что мы пыбрллм плохую хэш-функцию.

Математики разработали надежные (но очень сложные) хэш-  
функции, обладающие особыми свойствами:

1) хэш-код очень сильно меняется при малейшем изменении ис-  
ходных данных;

2) при известном хэш-коле т невозможно зп приемлемое время  
найти сообщение Af с таким хэш-кодом (//(АО - го);

3) при известном сообщении Л/ невозможно за приемлемое  
время найти сообщение Л/, с таким же хэш-кодом  
(ЖАО-ЖА/,)).

Здесь выражение «невозможно за приемлемое время» (или  
«вычислительно невозможно») означает, что эта задача решается  
только перебором вариантов (других алгоритмов не существует), а  
количество вариантов настолько велико, что на решение могут  
уйти сотни и тысячи лет. Поэтому даже если взломщик получил  
хэш-кол плроля, он не сможет за приемлемое время подучить сам  
пароль (или пароль, дающий такой же хэш-код).

Чем длиннее пароль, тем больше количество вариантов. Кро-  
ме длины для надёжности пароля важен используемый набор  
символов. Например, очень легко подбираются пароли, состоящие  
только из цифр. Если же пароль состоит из 10 символов и содер-  
жит латинские буквы (заглавные и строчные) и цифры, перебор  
вариантов (англ. brute force — метод «грубой силы») со скоростью  
10 мл и паролей и секунду займет более 2000 лет.

Нпдёжныс пароли должны состоять не менее чем из 7-8 сим-  
волов; пароли, состоящие из 15 символов и более, взломать мето-  
дом «грубой силы» практически невозможно. Не используйте па-  
роли типа «12345», «qwerty», свой день рождения, номер теле-  
фона. Плохо, если пароль представляет собой известное слово,  
для этих случаев взломщики используют подбор по словарю.  
Сложнее всего подобрать пароль, который представляет собой  
случайный набор заглавных и строчных букв, цифр и других  
знаков1.

Сегодня для хэширования в большинстве случаев применяют  
алгоритмы MD5, SHA1 и российский алгоритм, изложен мы й п  
ГОСТ Р34.11-94 (он считается одним из самых надёжных).  
В криптографии хэш-коды чаще всего имеют длину 128, 160 и  
256 битов.

Хэширование используется также для проверки правильности  
передачи данных: различные контрольные суммы — это не что  
иное, как хэш-коды.

Современные алгоритмы шифрования

Государстиеиным стандартом шифрования в России является  
алгоритм, зарегистрированный как ГОСТ 28147-89. Он является  
блочным шифром, г. е. шифрует не отдельные символы, в 64-бит-

иые блоки. В алгоритме предусмотрены 32 цикла преобразовании  
данных с 256-бмтиым ключом, за счёт этого он очень надёжен (об-  
ладает высокой криптостойкостью). На современных компьюте-  
рах раскрытие этого шифра путём переборе ключей («методом  
грубой силы») займёт не менее сотен лет, что делает такую атаку  
бессмысленной.

В США в качестве стандарта принят блочный шифр AES  
(англ. Advanced Encryption Standard, передовой стандарт шифро-  
вания), выбранный в 2001 г. по результатам проведённого кон-  
курса. Шифр AES используется также в защищенных беспровод-  
ных сетях (WiFi).

В Интернете популярен алгоритм RSA. названный так по на-  
чальным буквам фамилий его авторов — Р. Рай веста (R. Rivest),  
А. Шамира (A. Shamir) и JI. Адлемана (L. Adleman). ?>го алго-  
ритм с открытым ключом, стойкость алгоритма основана на том,  
что перемножить два очень больших простых числа достаточно  
просто, а вот разложить такое произведение на простые сомножи-  
тели очень трудно (эту задачу сейчас умеют решать только пере-  
бором вариантов). Поскольку количество вариантов огромно, для  
раскрытия шифра требуется много лет работы современных ком-  
пьютеров.

Для применения алгоритма RSA требуется построить откры-  
тый и секретный ключи следующим образом.

1. Выбрать два больших простых числа, р и q.

2. Найти их произведение п = рq и значение у-(р-1)-(7-1).

3. Выбрать число е (l<e<q>), которое ие имеет общих делите-  
лей с <р.

4. Найти число d, которое удовлетворяет условиюd-e-Агф + 1 для  
некоторого целого к.

5. Пара значений (е. л) — это открытый ключ RSA (его можно  
свободно публиковать), а пара (d, п) — это секретный ключ.  
Передаваемое сообщение нужно сначала представить в виде

последовательности чисел в интервале от 0 до п - 1. Для шифро-  
вания используют формулу  
у — х" mod п,

где х — исходное сообщение (число), (е.п) — открытый ключ,  
у — закодированное сообщение (число), а запись xr mod п обозна-  
чает остаток от деления х’ на п. Расшифровка сообщения выпол-  
няется по формуле  
х — у\* mod п.

Эти значит, что зашифровать сообщение может каждый (от-  
крытый ключ общеизвестен), а прочитать его — только тот, кто  
знает секретный показатель степени d.

Для лучшего понимания мы покажем работу алгоритма RSA  
на простом примере. Возьмём р-3 и 7-7, тогда находим  
л = р-7 = 21 и ,» = (р-1) (7-1) = 12. Выберем е = 5, тогда равенство  
d e = Лкр + 1 выполняется, например, при d = 17 (и Аг = 7). Таким об-  
разом. мы получили открытый ключ (5, 21) и секретный ключ  
(17. 21).

Зашифруем сообщение, состоящее из чисел 1, 2 и з, с помощью  
открытого ключа (5,21). получаем:

1 =ъ Р mod 21 - 1, 2=\*2bmod21 - 11, 3 => З1 mod 21 - 12.

т. е. зашифрованное сообщение состоит из чисел 1, 11 и 12. Зная  
секретный ключ (17, 21), можно его расшифровать:

1 =э l77mod21 - 1. 11 =э II17 mod 21 -2. 12 => 1217 mod 21 - 3.

Мы получили исходное сообщение.

Конечно, иы заметили, что при шифровании и расшифровке  
приходится вычислять остаток от деления очень больших чисел  
(например. 1217) на л. Оказывается, само число 1217 в этом случае  
находить не нужно. Достаточно записать в обычную целочислен-  
ную переменную, например лг, единицу, а потом 17 раз выполнить  
преобразование х - 12-х mod 21. После этого в переменной х бу-  
дет значение 12,т mod 21 - 3. Попробуйте доказать правильность  
этого алгоритма.

Чтобы взломать шифр, злоумышленнику надо узнать секрет-  
ный показатель степени d. А для этого необходимо найти боль-  
шие простые числа р и q, такие что n = p q. Если л велико, это  
очень сложная задача, её решение пе|юбором вариантов на совре-  
менном компьютере займёт сотни лет. В 2009 г. группа ученых из  
разных стран в результате многомесячных расчётов на сотнях  
компьютеров смогла расшифровать сообщение, зашифрованное  
алгоритмом RSA с 768-битным ключом. Поэтому сейчас надёж-  
ными считаются ключи с длиной 1024 битв и более. Если будет  
построен работающий квантовый компьютер, взлом алгоритма  
RSA будет возможен за очень небольшое время.

При использовании симметричных шифров всегдя возникает  
проблема: как передать ключ, если канал связи ненадёжный?  
Ведь, получив ключ, противник сможет расшифровать псе даль-  
нейшие сообщения. Для алгоритма RSA этой проблемы нет, сто-

ронам достаточно обменяться открытыми ключами, которые  
можно показывать всем желающим.

У алгоритма KSA есть еще одно достоинство: его можно ис-  
пользовать для цифровой подписи сообщений. Она служит для до-  
казательства авторства документов, защиты сообщений от поддел-  
ки и умышленных изменений.

Цифровая подпись — это набор символов, который получен  
в результате шифрования сообщения с помощью личного  
секретного кода отправителя.

Отправитель может передать вместе с исходным сообщением  
такое же сообщение, зашифрованное с помощью своего секретного  
ключа (это и есть цифровая подпись). Получатель расшифровыва-  
ет цифровую подпись с помощью открытого ключа. Если она со-  
впала с незашифрованным сообщением, можно быть уверенным,  
что его отправил тот человек, который знает секретный код. Если  
сообщение было изменено при передаче, оно не совпадёт с рас-  
шифрованной цифровой подписью. Так как сообщение может  
быть очень длинным, для сокращения объёма передаваемых дан-  
ных чаще всего шифруется не всё сообщение, а только его хэш-код.

Во многих современных программах есть возможность шифро-  
вать данные с паролем. Например, офисные пакеты OpenOffice.org  
и Microsoft Office позволяют шифровать все создаваемые доку-  
менты (для их просмотра и/или изменения нужно ввести пароль).  
При создании ирхиаа (например, в архиваторах Цл». ^WinRAR.

VVinZip) также можно установить пароль, без которого из-  
влечь файлы невозможно.

В простейших задачах для шифрования файлоп можно ис-  
пользовать бесплатную программу Шифровальщик (www.  
fnmilytree.ru/ru/cipher.htm). версии которой существуют для  
Linux и Windows. Программы Q TrueCrypt ([www.truecrypt.org](http://www.truecrypt.org)),  
BeatCrypt ([www.Jetlco.com](http://www.Jetlco.com)) и FrceOTFK (freeotfe.org) создают ло-  
гические диски-контейнеры, информация на которых шифрует-  
ся. Свободно распространяемая программа jjjj£ DlskCryptor  
(diskcryptor.net) позволяет шифровать разделы жестких дисков  
и даже создавать шифрованные флэш-диски и диски CD/DVD.

Программа ^ GnuPG (gnupg.org) также относится к свободно-  
му программному обеспечению. В ней поддерживаются симмет-  
ричные и несимметричные шифры, а также различные алгорит-  
мы электронной цифровой подписи.

Стенография

При передаче сообщений можно не только применять шифро-  
вание, но и скрывать сам факт передачи сообщения.

Стеганография — это наука о скрытой передаче информации  
путём скрытия самого факта передачи информации.

Древнегреческий историк Геродот описывал, нпнример. такой  
метод: на бритую голову раба записывалось сообщение, а когда  
его волосы отрастали, он отправлялся к получателю, который  
брил его голову и читал сообщение.

Классический метод стеганографии — симпатические (неви-  
димые) чернила, которые проявляются только при определенных  
условиях (нагрев, освещение, химический проявитель). Напри-  
мер, текст, написанный молоком, можно прочитать при нагреве.

Сейчас стеганография занимается скрытием информации в  
текстовых, графических. звуковых и видеофайлах с помощью  
программного «внедрения» в них нужных сообщений.

Простейшие способ — заменять младшие биты файла, в кото-  
ром закодировано изображение. Причем ото нужно сделать так,  
чтобы разница между исходным и полученным рисунками была  
неощутима для человека. Например, в чёрно-белом рисунке  
(266 оттенков серого) яркость каждого пикселя кодируется 8 би-  
тами. Если поменять 1-2 младших бита этого кода, «встроив»  
туда текстовое сообщение, фотография, в которой нет чётких гра-  
ниц. почти не изменится. При замене одного бита каждый байт  
исходного текстового сообщения хранится в младших битах кодов  
8 пикселей. Например, пусть первые 8 пикселей рисунка имеют  
такие коды:

10101101 1ОО101 ooiooi0101 <' I • 1 < 11 Ml) 1 о 1010101010101010 1010101 ! 10101111

Чтобы закодировать в них код буквы «И» (110010002), нужно  
изменить младшие биты кодов:

lioioitoljiooioiniooioioiijpioiooiojroioioil 1010101 OlOlOlOlBU 0101 но  
1 1 О О 1 0 0 о

Получателю нужно взять эти младшие биты и «собрать» их  
вместе в один байт.

Для звуков используются другие методы стеганографии, осно-  
ванные на добавлении п запись коротких условных сигналов, ко-  
торые обозначают 1 и О и не воспринимаются человеком на слух.  
Возможна также замена одного фрагмента звука на другой.

Для подтверждения авторства и охраны авторских прав на  
изображения, видео и звуковые файлы применяют цифровые во  
дяные знаки — внедрённую п файл информацию об авторе. Они  
получили своё название от старых водяных знаков на деньгах и  
документах. Для того чтобы установить авторство фотографии,  
достаточно расшифровать скрытую информацию, записанную с  
помощью водяного знака.

Иногда цифровые водяные знаки делают видимыми (текст  
или логотип компании на фотографии или на каждом кадре  
видеофильма). На многих сайтах, занимающихся продажей циф-  
ровых фотографий, видимые водяные знаки размещены на фото-  
графиях, предназначенных для предварительного просмотра.

Вопросы для теста

Параметр алгоритма шифрования (ключ)

Наука о способах шифрования информации (криптография, криптоанализ,шифрованиеб криптология)

Шифр, в котором для шифрования и расшифровки используется один и тот же ключ(Симметричный)

Функция, которая любое сообщение длины М переводит в короткий код m(Хэш-функция)

Каким видом шифрования является хэширование?(необратимое,с открытм ключом, обратимое, симметричное)

Как называется ситуация совпадения хэш-кодов различных строк (коллизия)

Свойства пароля, влияющие на его надежность(длина, набор символов, количество цифр)

Современные алгоритмы для хэширования (md5,sha1,rts,bruteforce)

Набор символов, который получен в результате шифрования сообщения с помощью личного секретного кода отправителя(цифровая подпись)

Наука о скрытой передачи информации (стенография, стереография, шифрование, криптография)

Какие знаки внедряются на изображение, видео, аудио для охраны авторских прав(цифровые водяные, водяные, лицензионные)