Шифрование - метод защиты информации

Испокон веков не было ценности большей, чем информация. XX век - век информатики и информатизации. Технология дает возможность передавать и хранить все большие объемы информации. Это благо имеет и оборотную сторону. Информация становится все более уязвимой по разным причинам:

- возрастающие объемы хранимых и передаваемых данных;
- расширение круга пользователей, имеющих доступ к ресурсам ЭВМ, программам и данным;
- усложнение режимов эксплуатации вычислительных систем.

Поэтому все большую важность приобретает проблема защиты информации от несанкционированного доступа (НСД) при передаче и хранении. Сущность этой проблемы - постоянная борьба специалистов по защите информации со своими "оппонентами".

Характеристики составных алгоритмов шифрования

Название алгоритма	Размер ключа, бит	Размер блока, бит	Размер вектора инициализации, бит	Количество циклов шифрования
Lucipher	128	128		
DES	56	64	64	16
FEAL-1	64	64	4	
B-Crypt	56	64	64	
IDEA	128	64		
ГОСТ 28147-89	256	64	64	32

Защита информации - совокупность мероприятий, методов и средств, обеспечивающих:

- исключение НСД к ресурсам ЭВМ, программам и данным;
- проверку целостности информации;
- исключение несанкционированного использования программ (защита программ от копирования).

- Очевидная тенденция к переходу на цифровые методы передачи и хранения информации позволяет применять унифицированные методы и алгоритмы для защиты дискретной (текст, факс, телекс) и непрерывной (речь) информации.

  Испытанный метод защиты информации от НСД - шифрование (криптография). ***Шифрованием*** (encryption) называют процесс преобразования открытых данных (plaintext) в зашифрованные (шифртекст, ciphertext) или зашифрованных данных в открытые по определенным правилам с применением ключей. В англоязычной литературе зашифрование/расшифрование - enciphering/deciphering.

С помощью криптографических методов возможно:

- шифрование информации;
- реализация электронной подписи;
- распределение ключей шифрования;
- защита от случайного или умышленного изменения информации.

К алгоритмам шифрования предъявляются определенные требования:

- высокий уровень защиты данных против дешифрования и возможной модификации;
- защищенность информации должна основываться только на знании ключа и не зависеть от того, известен алгоритм или нет (правило Киркхоффа);
- малое изменение исходного текста или ключа должно приводить к значительному изменению шифрованного текста (эффект "обвала");
- область значений ключа должна исключать возможность дешифрования данных путем перебора значений ключа;
- экономичность реализации алгоритма при достаточном быстродействии;
- стоимость дешифрования данных без знания ключа должна превышать стоимость данных.

- Перед шифрованием информацию следует подвергнуть статистическому кодированию (сжатию, архивации). При этом уменьшится объем информации и ее избыточность, повысится энтропия (среднее количество информации, приходящееся на один символ). Так как в сжатом тексте будут отсутствовать повторяющиеся буквы и слова, дешифрование (криптоанализ) затруднится.

Классификация алгоритмов шифрования

- 1. Симметричные (с секретным, единым ключом, одноключевые, single-key).
  1.1. Потоковые (шифрование потока данных):

с одноразовым или бесконечным ключом (infinite-key cipher);

с конечным ключом (система Вернама - Vernam);

на основе генератора псевдослучайных чисел (ПСЧ).

1.2. Блочные (шифрование данных поблочно):
1.2.1. Шифры перестановки (P-блоки);
1.2.2. Шифры замены (S-блоки):

моноалфавитные (код Цезаря);

полиалфавитные (шифр Виджженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma);

1.2.3. составные :

Lucipher (фирма IBM, США);
DES (Data Encryption Standard, США);
FEAL-1 (Fast Enciphering Algoritm, Япония);
IDEA/IPES (International Data Encryption Algorithm/
Improved Proposed Encryption Standard, фирма Ascom-Tech AG, Швейцария);
B-Crypt (фирма British Telecom, Великобритания);
ГОСТ 28147-89 (СССР); * Skipjack (США).

- 2. Асимметричные (с открытым ключом, public-key):

Диффи-Хеллман DH (Diffie, Hellman);
Райвест-Шамир-Адлеман RSA (Rivest, Shamir, Adleman);
Эль-Гамаль ElGamal.

- Кроме того, есть разделение алгоритмов шифрования на собственно шифры (ciphers) и коды (codes). Шифры работают с отдельными битами, буквами, символами. Коды оперируют лингвистическими элементами (слоги, слова, фразы).

Симметричные алгоритмы шифрования

- Симметричные алгоритмы шифрования (или криптография с секретными ключами) основаны на том, что отправитель и получатель информации используют один и тот же ключ. Этот ключ должен храниться в тайне и передаваться способом, исключающим его перехват.

Обмен информацией осуществляется в 3 этапа:

- отправитель передает получателю ключ (в случае сети с несколькими абонентами у каждой пары абонентов должен быть свой ключ, отличный от ключей других пар);
- отправитель, используя ключ, зашифровывает сообщение, которое пересылается получателю;
- получатель получает сообщение и расшифровывает его.
- Если для каждого дня и для каждого сеанса связи будет использоваться уникальный ключ, это повысит защищенность системы.

Потоковые шифры

- В потоковых шифрах, т. е. при шифровании потока данных, каждый бит исходной информации шифруется независимо от других с помощью гаммирования.

  Гаммирование - наложение на открытые данные гаммы шифра (случайной или псевдослучайной последовательности единиц и нулей) по определенному правилу. Обычно используется "исключающее ИЛИ", называемое также сложением по модулю 2 и реализуемое в ассемблерных программах командой XOR. Для расшифровывания та же гамма накладывается на зашифрованные данные.

  При однократном использовании случайной гаммы одинакового размера с зашифровываемыми данными взлом кода невозможен (так называемые криптосистемы с одноразовым или бесконечным ключом). В данном случае "бесконечный" означает, что гамма не повторяется.

  В некоторых потоковых шифрах ключ короче сообщения. Так, в системе Вернама для телеграфа используется бумажное кольцо, содержащее гамму. Конечно, стойкость такого шифра не идеальна.

  Понятно, что обмен ключами размером с шифруемую информацию не всегда уместен. Поэтому чаще используют гамму, получаемую с помощью генератора псевдослучайных чисел (ПСЧ).

Блочные шифры

При блочном шифровании информация разбивается на блоки фиксированной длины и шифруется поблочно. Блочные шифры бывают двух основных видов:

- шифры перестановки (P-блоки);
- шифры замены (S-блоки).

Шифры перестановок переставляют элементы открытых данных (биты, буквы, символы) в некотором новом порядке. Различают шифры горизонтальной, вертикальной, двойной перестановки, решетки, лабиринты, лозунговые и др.

Шифры замены заменяют элементы открытых данных на другие элементы по определенному правилу. Различают шифры простой, сложной, парной замены, буквенно-слоговое шифрование и шифры колонной замены. Шифры замены делятся на две группы:

- моноалфавитные (код Цезаря) ;
- полиалфавитные (шифр Видженера, цилиндр Джефферсона, диск Уэтстоуна, Enigma).

- В моноалфавитных шифрах замены буква исходного текста заменяется на другую, заранее определенную букву. Например в коде Цезаря буква заменяется на букву, отстоящую от нее в латинском алфавите на некоторое число позиций. Очевидно, что такой шифр взламывается совсем просто. Нужно подсчитать, как часто встречаются буквы в зашифрованном тексте, и сопоставить результат с известной для каждого языка частотой встречаемости букв.

- В полиалфавитных подстановках для замены некоторого символа исходного сообщения в каждом случае его появления последовательно используются различные символы из некоторого набора. Понятно, что этот набор не бесконечен, через какое-то количество символов его нужно использовать снова. В этом слабость чисто полиалфавитных шифров.

- В современных криптографических системах, как правило, используют оба способа шифрования (замены и перестановки). Такой шифратор называют составным (product cipher). Он более стойкий, чем шифратор, использующий только замены или перестановки.

- Блочное шифрование можно осуществлять двояко :
- 1. Без обратной связи (ОС). Несколько битов (блок) исходного текста шифруются одновременно, и каждый бит исходного текста влияет на каждый бит шифртекста. Однако взаимного влияния блоков нет, то есть два одинаковых блока исходного текста будут представлены одинаковым шифртекстом. Поэтому подобные алгоритмы можно использовать только для шифрования случайной последовательности битов
- 2. С обратной связью. Обычно ОС организуется так: предыдущий шифрованный блок складывается по модулю 2 с текущим блоком. В качестве первого блока в цепи ОС используется инициализирующее значение. Ошибка в одном бите влияет на два блока - ошибочный и следующий за ним.

Генератор ПСЧ может применяться и при блочном шифровании :

1. Поблочное шифрование потока данных. Шифрование последовательных блоков (подстановки и перестановки) зависит от генератора ПСЧ, управляемого ключом.
2. Поблочное шифрование потока данных с ОС. Генератор ПСЧ управляется шифрованным или исходным текстом или обоими вместе.

Весьма распространен федеральный стандарт США DES (Data Encryption Standard) , на котором основан международный стандарт ISO 8372-87. DES был поддержан Американским национальным институтом стандартов (American National Standards Institute, ANSI) и рекомендован для применения Американской ассоциацией банков (American Bankers Association, ABA). DES предусматривает 4 режима работы:

- ECB (Electronic Codebook) электронный шифрблокнот;
- CBC (Cipher Block Chaining) цепочка блоков;
- CFB (Cipher Feedback) обратная связь по шифртексту;
- OFB (Output Feedback) обратная связь по выходу.

- ГОСТ 28147-89 - отечественный стандарт на шифрование данных . Стандарт включает три алгоритма зашифровывания (расшифровывания) данных: режим простой замены, режим гаммирования, режим гаммирования с обратной связью - и режим выработки имитовставки.

- С помощью имитовставки можно зафиксировать случайную или умышленную модификацию зашифрованной информации. Вырабатывать имитовставку можно или перед зашифровыванием (после расшифровывания) всего сообщения, или одновременно с зашифровыванием (расшифровыванием) по блокам. При этом блок информации шифруется первыми шестнадцатью циклами в режиме простой замены, затем складывается по модулю 2 со вторым блоком, результат суммирования вновь шифруется первыми шестнадцатью циклами и т. д.

- Алгоритмы шифрования ГОСТ 28147-89 обладают достоинствами других алгоритмов для симметричных систем и превосходят их своими возможностями. Так, ГОСТ 28147-89 (256-битовый ключ, 32 цикла шифрования) по сравнению с такими алгоритмами, как DES (56-битовый ключ, 16 циклов шифрования) и FEAL-1 (64-битовый ключ, 4 цикла шифрования) обладает более высокой криптостойкостью за счет более длинного ключа и большего числа циклов шифрования.

- Достоинствами ГОСТ 28147-89 являются также наличие защиты от навязывания ложных данных (выработка имитовставки) и одинаковый цикл шифрования во всех четырех алгоритмах ГОСТа.

Асимметричные алгоритмы шифрования

- В асимметричных алгоритмах шифрования (или криптографии с открытым ключом) для зашифровывания информации используют один ключ (открытый), а для расшифровывания - другой (секретный). Эти ключи различны и не могут быть получены один из другого.

- Схема обмена информацией такова:
- получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным (сообщает отправителю, группе пользователей сети, публикует);
- отправитель, используя открытый ключ получателя, зашифровывает сообщение, которое пересылается получателю;
- получатель получает сообщение и расшифровывает его, используя свой секретный ключ.
- RSA [4, 5]
- Защищен патентом США N 4405829. Разработан в 1977 году в Массачусетском технологическом институте (США). Получил название по первым буквам фамилий авторов (Rivest, Shamir, Adleman). Криптостойкость основана на вычислительной сложности задачи разложения большого числа на простые множители.
- ElGamal
- Разработан в 1985 году. Назван по фамилии автора - Эль-Гамаль. Используется в стандарте США на цифровую подпись DSS (Digital Signature Standard). Криптостойкость основана на вычислительной сложности задачи логарифмирования целых чисел в конечных полях

Сравнение симметричных и асимметричных алгоритмов шифрования

- В асимметричных системах необходимо применять длинные ключи (512 битов и больше). Длинный ключ резко увеличивает время шифрования. Кроме того, генерация ключей весьма длительна. Зато распределять ключи можно по незащищенным каналам.

  В симметричных алгоритмах используют более короткие ключи, т. е. шифрование происходит быстрее. Но в таких системах сложно распределение ключей.

  Поэтому при проектировании защищенной системы часто применяют и симметричные, и асимметричные алгоритмы. Так как система с открытыми ключами позволяет распределять ключи и в симметричных системах, можно объединить в системе передачи защищенной информации асимметричный и симметричный алгоритмы шифрования. С помощью первого рассылать ключи, вторым же - собственно шифровать передаваемую информацию [4, с. 53].

  Обмен информацией можно осуществлять следующим образом:
- получатель вычисляет открытый и секретный ключи, секретный ключ хранит в тайне, открытый же делает доступным;
- отправитель, используя открытый ключ получателя, зашифровывает сеансовый ключ, который пересылается получателю по незащищенному каналу;
- получатель получает сеансовый ключ и расшифровывает его, используя свой секретный ключ;
- отправитель зашифровывает сообщение сеансовым ключом и пересылает получателю;
- получатель получает сообщение и расшифровывает его.
- Надо заметить, что в правительственных и военных системах связи используют лишь симметричные алгоритмы, так как нет строго математического обоснования стойкости систем с открытыми ключами, как, впрочем, не доказано и обратное.

Литература

- 1. Водолазский В. Коммерческие системы шифрования: основные алгоритмы и их реализация. Часть 1. // Монитор. - 1992. - N 6-7. - с. 14 - 19.
- 2. Игнатенко Ю.И. Как сделать так, чтобы?.. // Мир ПК. - 1994. - N 8. - с. 52 - 54.
- 3. Ковалевский В., Максимов В. Криптографические методы. // КомпьютерПресс. - 1993. - N 5. - с. 31 - 34.
- 4. Мафтик С. Механизмы защиты в сетях ЭВМ. - М.: Мир, 1993.
- 5. Спесивцев А.В., Вегнер В.А., Крутяков А.Ю. и др. Защита информации в персональных ЭВМ. - М.: Радио и связь, 1992.
- 6. Сяо Д., Керр Д., Мэдник С. Защита ЭВМ. - М.: Мир, 1982.
- 7. Шмелева А. Грим - что это ? // Hard'н'Soft. - 1994. - N 5.
- 8. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.