электронное научно-техническое издание
НАУКА и ОБРАЗОВАНИЕ
Эл № ФС 77 - 30569. Государственная регистрация №0421100025. ISSN 1994-0408

Симметричное шифрование (гаммирование)

 # 03, март 2011

автор: Гончаров Н. О.

МГТУ им. Н.Э. Баумана
goncharovkolya@list.ru

Введение

Целью работы является изучение симметричного шифрования (гаммирования), которое считается одним из самых высокопроизводительных методов для защиты информации, рассмотрение известных блочных шифров, общей схемы, и принципов работы шифрования, разработка программного обеспечения по реализации алгоритма шифрования, основанного на гаммировании.

Криптография в прошлом использовалась лишь в военных целях. Однако сейчас, по мере образования информационного общества, криптография становится одним из основных инструментов, обеспечивающих конфиденциальность, авторизацию, электронные платежи, корпоративную безопасность и бесчисленное множество других важных вещей.

Криптографические методы могут применяться для решений следующих проблем безопасности: конфиденциальность передаваемых/хранимых данных; аутентификация; целостности хранимых и передаваемых данных; обеспечение подлинности документов. Так же эти методы применяются в базовых метода преобразования информации, которыми являются: шифрование (симметричное и несимметричное); вычисление хэш функций; генерация электронной цифровой подписи; генерация последовательности псевдослучайных чисел.

Шифрование – это обратимое преобразование данных с целью их сокрытия от посторонних. Почти все методы шифрования используют ключ шифрования – секретную кодовую последовательность, используемую в процессе преобразования информации.

Методов шифрования было придумано множество – от шифров простой замены (наиболее известный пример – «Пляшущие человечки» Конан Дойля) до принципиально невскрываемого шифра Вернама (двоичное сложение исходного текста с однократно используемой случайной последовательностью).

Классическими шифрами принято называть симметричные блочные шифры, которые для шифрования и дешифрования информации используют один и тот же ключ и шифруют информацию блоками. Длина блока обычно составляет 8 или 16 байт. Есть алгоритмы, допускающие переменную длину блока.

Самыми известными блочными шифрами являются отечественный шифр, определённый стандартом ГОСТ 28147-89 и американский стандарт *DES* (*Data Encryption Standard*), у которых длина блока *n* равна 64 и 256 соответственно.

Необходимо отметить, что кроме блочных шифров существуют и активно используются поточные шифры. Они, как и блочные шифры, используют симметричный ключ, но выполняют шифрования входного потока побайтно или, иногда, побитно. Идея поточного шифра состоит в том, что на основе симметричного ключа вырабатывается ключевая последовательность (гамма–последовательность), которая складывается по модулю два (операция *xor*) с входным потоком. Поточные шифры, как правило, более производительны, чем блочные и используются для шифрования речи.

Термин гамма-последовательность (*gamma sequence*) обычно употребляется в отношении последовательности псевдослучайных элементов, которые генерируются по определенному закону и алгоритму.

В процессе выполнения работы выполнен анализ известных данных о методах симметричного шифрования. Рассмотрен метод классического шифрования Шеннона [1], блочные шифры - американский шифр *DES* [2] и отечественный шифр, определённый стандартом ГОСТ 28147-89, *IDEA* (*International Data Encryption Algorithm*), *CAST*, Шифр *Skipjack, RC2* и *RC4* и др. [3]

Кроме того, выполнена опытно-экспериментальная работа по разработке программного обеспечения по реализации алгоритма шифрования, основанного на гаммировании. Используя при этом язык объектно-ориентированного программирования Visual Basic [4].

1. Симметричное шифрование (гаммирование)

Симметричное шифрование - это метод шифрования, при котором для защиты информации используется ключ, зная который любой может расшифровать или зашифровать данные [2].

Алгоритмы с симметричными ключами имеют очень высокую производительность. Криптография с симметричными ключами стойкая, что делает практически невозможным процесс дешифрования без знания ключа. При прочих равных условиях стойкость определяется длиной ключа. Так как для шифрования и дешифрования используется один и

тот же ключ, при использовании таких алгоритмов требуются высоко надежные механизмы для распределения ключей. Ещё одна проблемой является безопасное распространение симметричных ключей. Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных.

Гаммированием (*gamma xoring*) называется процесс «наложения» гамма-последовательности на открытые данные. Обычно это суммирование по какому-либо модулю, например, по модулю два, такое суммирование принимает вид обычного «исключающего ИЛИ» суммирования.

Симметричное шифрование остаётся самым актуальным и криптографически гарантированными методом защиты информации. В симметричном шифровании, основанном на использовании составных ключей, идея состоит в том, что секретный ключ делится на две части, хранящиеся отдельно. Каждая часть сама по себе не позволяет выполнить дешифрование.

Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю. Это создает проблему распространения ключей. Получатель на основании наличия зашифрованного и расшифрованного сообщения не может доказать, что он получил это сообщение от конкретного отправителя, поскольку такое же сообщение он мог сгенерировать самостоятельно. Схема распределения ключей представлена на рисунке 1.

Рисунок 1. Схема распределения ключей при симметричном шифровании

2. Схемы и принципы симметричного шифрования

В общедоступной литературе математические задачи криптографии на современном уровне впервые были рассмотрены К. Шенноном в работе [1], хотя по некоторым данным в России аналогичные результаты были известны и раньше. В этой работе К. Шеннон с помощью предложенного им теоретико-информационного подхода решил некоторые из важнейших проблем теоретико-информационной криптографии. В частности, им показано, что абсолютной надежностью могут обладать только те шифры, у которых объем ключа не меньше объема шифруемой информации, а также приведены примеры таких шифров. Там же были предложены и принципы построения криптографически надежных преобразований с помощью композиции некоторых разнородных отображений и т. п.

В указанной работае Шеннона были сформулированы и доказаны математическими средствами необходимые и достаточные условия недешифруемости системы шифра. Было установлено, что единственным недешифруемым шифром является, так называемая, лента одноразового использования (*One-time Pad*), когда открытый текст шифруется с помощью случайного ключа такой же длины. Это обстоятельство делает абсолютно стойкий шифр очень дорогим в эксплуатации.

Прежде всего, Шеннон сделал вывод, что во всех, даже очень сложных шифрах, в качестве типичных компонентов можно выделить шифры замены и перестановки.

Математическое описание шифра замены выглядит следующим образом. Пусть $\boldsymbol{X}$ и $\boldsymbol{Y}$ - два текста (открытый и шифрованный соответственно), $\boldsymbol{X}$ взаимно однозначно отображается в текст $\boldsymbol{Y}$. Действие шифра замены можно представить как преобразование открытого текста $\boldsymbol{X = (x_1,x_2,\ldots x_n)}$ в шифрованныйтекст $\boldsymbol{Y = g(X)=g(x_1,x_2,\ldots,x_n).}$

Математическое описание шифра перестановки выглядит следующим образом. Пусть длина отрезков, на которые разбивается открытый текст, равна $\boldsymbol{m}$, а $\boldsymbol{S}$ - взаимно однозначное отображение $\boldsymbol{X = (x_1,x_2,\ldots x_m)}$ в себя. Шифр перестановки преобразует отрезок открытого текста $\boldsymbol{x_1,x_2,\ldots x_m}$ в отрезок шифрованного текста $\boldsymbol{S(x_1,x_2,\ldots,x_m)}$ (рисунок 2).

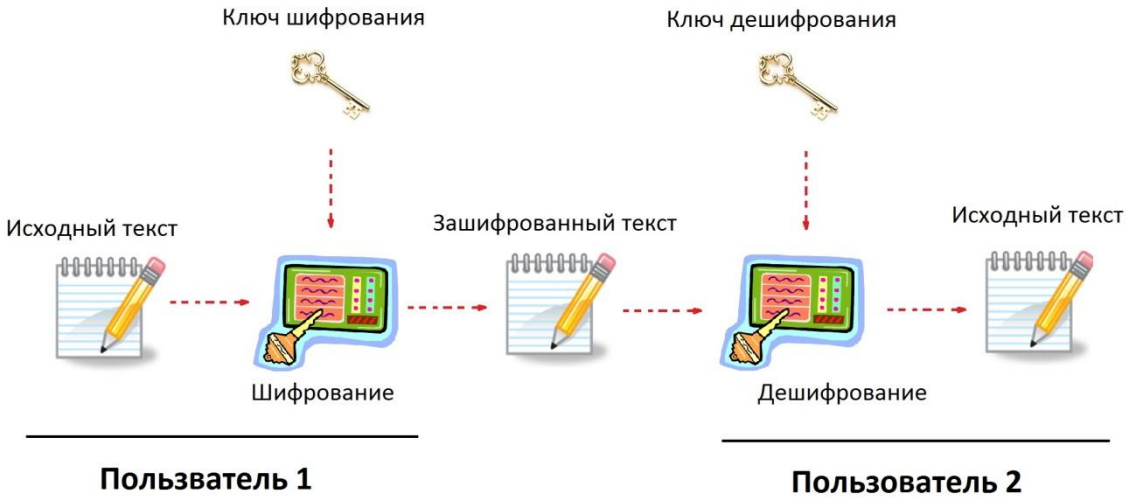

Рисунок 2. Общая схема шифрования

Абсолютно стойкие шифры преименяются в сетях связи с небольшим объемом передаваемой информации, которые используют, как правило, для передачи особо важной государственной информации. Это объясняется тем, что каждый передаваемый текст должен иметь свой собственный, единственный и неповторимый ключ. Следовательно, перед использованием этого шифра все абоненты должны быть обеспечены достаточным запасом случайных ключей и должна быть исключена возможность их повторного применения. Выполнение этих требований необычайно трудно и дорого.

При реализации с помощью вычислительной технике, как говорилось ранее, алгоритмы шифрования получили еще одну классификацию - их подразделяют на блочные и поточные.

Блочный шифр A_k представляет собой автомат, входами и выходами которого являются последовательности X и $\psi = A_k(X)$ длины n. Входная последовательность X разбивается на блоки длины n и каждый блок шифруется независимо один от другого одним ключем K.

Поточный шифр представляет собой автономный автомат, который вырабатывает псевдослучайную двоичную последовательность $\gamma = (\gamma_0,\ldots,\gamma_n\ldots)$. В качестве шифрованной информации выступает последовательность $\xi = (\xi_0,\ldots, \xi_n,\ldots)$. Обычно в качестве функции наложения ϕ используется функция сложения в каком либо конечном поле или кольце,

в частности, в двоичном случае $\xi = \beta \oplus \gamma$. В последнем случае обратное преобразование (дешифрование) осуществляется по формуле $\beta = \xi \oplus \gamma$, что позволяет на обоих концах канала связи иметь шифраторы с одинаковыми ключами.

Поточные шифры, как правило, более производительны, чем блочные и используются для шифрования речи, сетевого трафика и иных данных с заранее неизвестной длиной. При достаточно частой смене ключа для выработки гаммы - последовательности поточные шифры обеспечивают достаточную стойкость.

3. Классическое шифрование

Шифр *DES* работает следующим образом [2]. Данные представляются в цифровом виде и разбиваются на блоки длинной 64 бита, затем поблочно шифруются. Блок разбивается на левую и правую части. На первом этапе шифрования вместо левой части блока записывается правая, а вместо правой - сумма по модулю два левой и правой частей. На втором этапе по определенной схеме выполняются побитовые замены и перестановки. Ключ *DES* имеет длину 64 бита, из которых 56 битов - случайные, а 8 - служебные, используемые для контроля ключа.

IDEA [5] - блочный шифр с длиной ключа 128 бит. Этот европейский стандарт предложен в 1990 году. Шифр *IDEA* по скорости и стойкости к анализу не уступает шифру *DES*.

CAST [5] - это блочный шифр, использующий 128-битовый ключ в США и 40-битный - в экспортном варианте. *CAST* используется компанией *Northern Telecom (Nortel).*

Шифр *Skipjack* [5], разработанный Агентством национальной безопасности США *(National Security Agency - NSA),* использует 80-битовые ключи.

Шифры *RC2* и *RC4* [5] разработаны Роном Рейвестом - одним из основателей компании *RSA Data Security*, и запатентованы этой компанией. Они используют ключи разной длины, а в экспортируемых продуктах заменяют *DES*. Шифр *RC2* - блочный, с длиной блока 64 бита; шифр *RC4* - поточный. По замыслу разработчиков, производительность *RC2* и *RC4* должна быть не меньше, чем у алгоритма *DES*.

4. Асимметричное шифрование

В 1976 году была опубликована работа молодых американских математиков У. Диффи и М.Э. Хеллмана "Новые направления в криптографии" [6]. В данной работе центральными являются два определения: односторонняя функция и функция с секретом.

Односторонней называется функция $F(X)$, обладающая двумя свойствами: существует полиномиальный алгоритм вычисления значений $F(X)$, не существует полиномиального алгоритма инвертирования функции F. Иначе говоря, в этой функции расшифровка зашифрованного ею же текста не предусмотрена.

Функцией с секретом называется функция F_k зависящая от параметра k и обладающая следующими свойствами: существует полиномиальный алгоритм вычисления значения $F_k(X)$ для любых k и X; не существует полиномиального алгоритма инвертирования F_k при неизвестном k; существует полиномиальный алгоритм инвертирования F_k при известном k.

Шифрование при помощи функции с секретом получило также название асимметричного шифрования.

На рисунке 3 представлена блок-схема алгоритма шифрования, основанного на гаммировании.

Рисунок 3. Блок-схема алгоритма

На рисунке 4 представлена блок-схема полного алгоритма шифрования, основанного на гаммировании.

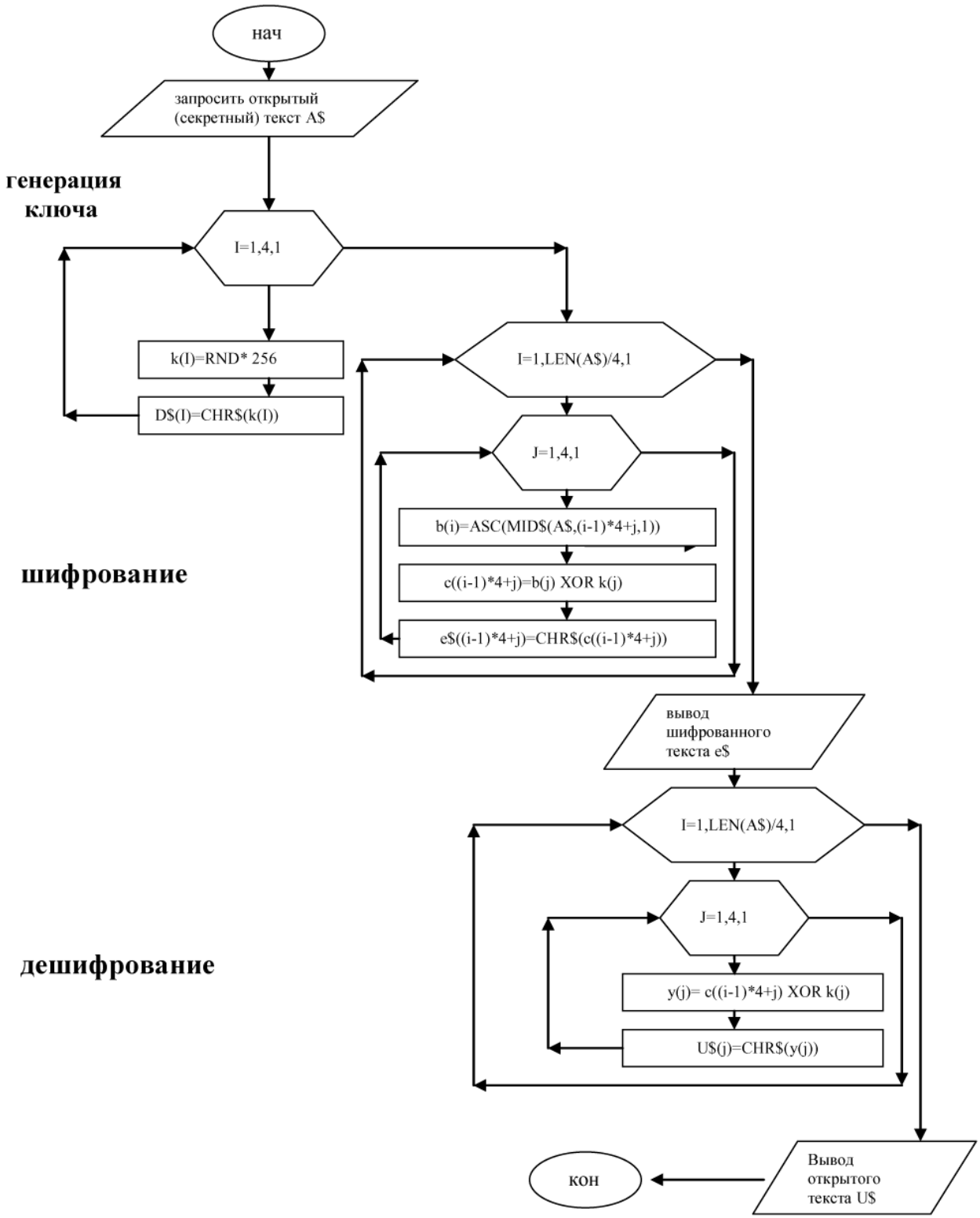

Рисунок 4. Блок-схема полного алгоритма

Заключение

Симметричное шифрование остаётся самым актуальным и криптографически гарантированным методом защиты информации. В симметричном шифрование, основанном на использовании составных ключей, идея состоит в том, что секретный ключ делится на две части, хранящиеся отдельно. Каждая часть сама по себе не позволяет выполнить дешифрование. Если у правоохранительных органов появляются подозрения относительно лица, использующего некоторый ключ, они могут в установленном порядке получить половинки ключа и дальше действовать обычным для симметричного дешифрования образом. Порядок работы с составными ключами - хороший пример следования принципу разделения обязанностей. Он позволяет сочетать права на разного рода тайны (персональную, коммерческую) с возможностью эффективно следить за нарушителями закона, хотя, конечно, здесь очень много тонкостей и технического, и юридического плана.

Алгоритмы с симметричными ключами имеют очень высокую производительность. Криптография с симметричными ключами очень стойкая, что делает практически невозможным процесс дешифрования без знания ключа. При прочих равных условиях стойкость определяется длиной ключа. Так как для шифрования и дешифрования используется один и тот же ключ, при использовании таких алгоритмов требуются очень надежные механизмы для распределения ключей.

Алгоритмы симметричного шифрования используют ключи не очень большой длины и могут быстро шифровать большие объемы данных.

Поточные шифры очень производительны, используются для шифрования речи, сетевого трафика и иных данных с заранее неизвестной длиной. При достаточно частой смене ключа для выработки гамма - последовательности поточные шифры обеспечивают достаточную стойкость.

Всем системам открытого шифрования присущи следующие основные недостатки: ключ должен передаваться по секретному каналу; к службе генерации ключей предъявляются повышенные требования, обусловленные тем, что для ***n*** абонентов при схеме взаимодействия "каждый с каждым" требуется ***n*(n-1)/2** ключей, то есть зависимость числа ключей от числа абонентов является квадратичной. Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю.

Проблемой, которая актуальна и для других криптосистем, является вопрос о том, как безопасно распространять симметричные (секретные) ключи.

В перспективах возможно: Осуществить передачу ключей на основе квантовой криптографии; разработать методы и их программно-аппаратную реализацию по увеличению длины псевдослучайной последовательности.

Литература:

1. Шеннон К. Э. Работы по теории информации и кибернетике, М.: ИЛ, 1963. 832 с.
2. А.В. Аграновский, Р.А. Хади. Практическая криптография (серия «Аспекты защиты»), М.: Солон-Пресс, 2002. 254 с.
3. Т.Л. Партыка, И.И. Попов. Информационная безопасность. М.: Форум-Инфра, 2007. 368 с.
4. С.В. Глушаков А.С.Сурядный. Программирование на Visual Basic 6. Х.: Фалио, 2004. 497с.
5. Брюс Шнайер. Прикладная криптография, 2е изд, изд.Триумф,2002. 816 с.
6. У.Диффи и М.Э.Хеллман. Новые направления в криптографии,1976 . 654 с.