Федеральное государственное казенное образовательное учреждение

высшего профессионального образования

**«Омская академия МВД России»**

|  |  |
| --- | --- |
| **Кафедра** | управления и информационных технологий  в деятельности органов внутренних дел |

|  |  |  |  |
| --- | --- | --- | --- |
| **Контрольная работа по дисциплине:** | | Основы информационной безопасности  в Органах Внутренних Дел | |
|  | |  | |
| **Тема:** | Современные стандарты шифрования развитых зарубежных стран. | | |
|  |  | | |
|  |  | | |
| **Выполнил:** | Слушатель ОмА МВД России | | |
|  | Участковый уполномоченный полиции | | (должность) |
|  | капитан полиции | | (звание) |
|  | Кузнецов Виталий Викторович | | (Ф.И.О.) |
|  |  | |  |
|  | ПФЗОП-522 | | аббревиатура учебной группы |
|  |  | |  |
| **Комплектующий орган:** | ОП «Заводской» Управления МВД России по г. Новокузнецку | | |
| **Контактный тел:** | 8-913-333-01-34 | | |
| **Email:** |  | | |

**ОМСК 2016 г.**

**Контрольный талон**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Дата поступления работы на кафедру | « | 7 | »12 | 2016\_ г. |  | Рег. № | 108 |

|  |
| --- |
|  |
|  |
|  |

|  |  |
| --- | --- |
| Результат проверки контрольной работы: |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Контрольную работу проверил: | | | | | | | |
|  | | | | | | | |
| (должность, ученая степень (ученое звание), инициалы, фамилия) | | | | | | | |
| Дата проверки работы | « |  | » | 201\_ г. |  |  |  | |

**Оглавление**

Введение...................................................................................................................3

1. Современные стандарты шифрования США……......................................4

2.Стандарты шифрования Японии…….. ......................................................10

Заключение……………………………………………………………………....13

Список использованной литературы...........................................................14

**Введение**

В настоящее время все больше людей начинают задумываться о своей безопасности. Люди все больше зависимы от компьютеров и все меньше знают о способах защиты своих личных данных от злоумышленников. Конечно, встает вопрос о том как защитить пользователей и как пользователь может защитить себя. Каждый специалист в сфере компьютерной безопасности может предложить свой способ обезопасить пользователей, используя алгоритмы шифрования. Наука, изучающая алгоритмы шифрования называется криптографией.

Криптография позволяет передавать информацию в защищенной форме, обеспечивая безопасность, конфиденциальность и целостность данных. При защите конфиденциальной информации криптография способствует высокому уровню безопасности персональных данных отдельных людей и групп. Доступ к информации, хранящейся в компьютерных базах данных, значительно возрос. Компании хранят корпоративные и персональные данные на компьютерах чаще, чем когда-либо ранее. Большая часть хранящейся информации строго конфиденциальна и не предназначена для публичного просмотра. Поэтому исследование вопросов, связанных со стандартами шифрования является весьма актуальным.

Цель контрольной работы – рассмотреть современные стандарты шифрования развитых зарубежных стран. В работе будут рассмотрены современные стандарты шифрования США и Японии.

**1. Современные стандарты шифрования США**

Процесс преобразования открытых данных в зашифрованные и наоборот принято называть шифрованием, причем две составляющие этого процесса называют соответственно зашифрованием и расшифрованием. Математически данное преобразование представляется следующими зависимостями, описывающими действия с исходной информацией:

С = Ek1(M)

<p>M' = Dk2(C),

где M (message) - открытая информация (в литературе по защите информации часто носит название "исходный текст");

C (cipher text) - полученный в результате зашифрования шифртекст (или криптограмма);

E (encryption) - функция зашифрования, выполняющая криптографические преобразования над исходным текстом;

k1 (key) - параметр функции E, называемый ключом зашифрования;

M' - информация, полученная в результате расшифрования;

D (decryption) - функция расшифрования, выполняющая обратные зашифрованию криптографические преобразования над шифртекстом;

k2 - ключ, с помощью которого выполняется расшифрование информации.

Стандарты по защите данных ЭВМ от несанкционированного доступа необходимы в таких областях, как шифрование, установление подлинности личности и данных (аутентификация), контроль доступа, надёжное хранение и передача данных

Алгоритмы шифрования можно разделить на две категории: симметричного и асимметричного шифрования. Для первых соотношение ключей зашифрования и расшифрования определяется как k1 = k2 = k (т. е. функции E и D используют один и тот же ключ шифрования). При асимметричном шифровании ключ зашифрования k1 вычисляется по ключу k2 таким образом, что обратное преобразование невозможно, например, по формуле k1 = ak2 mod p (a и p - параметры используемого алгоритма).

Рассмотрим стандарты шифрования США: алгоритмы шифрования DES и AES.

В 1977 г. был разработан алгоритм симметричного шифрования DES (Data Encryption Standard). До недавнего времени он был "стандартом США", поскольку правительство этой страны рекомендовало применять его для реализации различных систем шифрования данных. Несмотря на то, что изначально DES планировалось использовать не более 10-15 лет, попытки его замены начались только в 1997 г.

Алгоритм DES базируется на научной работе Шеннона 1949г., связавшей криптографию с теорией информации. Шеннон выделил два общих принципа, используемых в практических шифрах: рассеивание и перемещение. Рассеиванием он, назвал распространение влияния одного знака открытого текста на множество знаков шифртекста, что позволяет скрыть статистические свойства открытого текста. Под перемещением Шеннон понимал использование взаимосвязи статистических свойств открытого и шифрованного текстов. Но шифр должен не только затруднять раскрытие, а ещё обеспечивать лёгкость шифрования и дешифрования при известном секретном ключе. Поэтому была принята идея использовать произведение простых шифров, каждый из которых вносит небольшой вклад в значительное суммарное рассеивание и перемещение.

В составных шифрах в качестве элементарных составляющих чаще всего используются простые замены (подстановки) и перестановки. Все перестановки и коды в таблицах подобраны разработчиками таким образом, чтобы максимально затруднить процесс дешифрования текста путём подбора ключа.

Алгоритм DES строится в соответствии с методологией сетей Фейстеля и состоит из чередующейся последовательности перестановок и замен. Алгоритм DES осуществляет шифрование 64-битовых блоков данных с помощью 64-битового ключа, в котором значащими являются 56 бит (остальные 8 – проверочные биты для контроля на чётность).

Процесс шифрования состоит из: начальной перестановки битов 64-битового блока, 16 циклов (раундов) шифрования; конечной перестановки битов.

Процесс дешифрования результата работы алгоритма DES является инверсным к процессу шифрования. Все операции должны быть выполнены в обратном шифрованию порядке. Это означает, дешифруемые данные сначала переставляются в соответствии с матрицей обратной перестановки, а затем над последовательностью битов выполняются те же действия, что и в процессе шифрования, но в обратном порядке, и затем выполняется перестановка, обратная начальной.

Основные достоинства алгоритма DES:

- используется только один ключ длиной 56 бит;

- зашифровав сообщение с помощью одного пакета программ, для дешифрования можно использовать любой другой пакет программ, соответствующий стандарту DES;

- относительная простота алгоритма обеспечивает высокую скорость обработки;

- криптостойкость алгоритма вполне достаточна для обеспечения информационной безопасности большинства коммерческих приложений.

Прямым развитием DES в настоящее время является алгоритм [Triple DES](https://ru.wikipedia.org/wiki/3DES) (3DES). В 3DES шифрование/расшифровка выполняются путём троекратного выполнения алгоритма DES.

[Triple DES](https://ru.wikipedia.org/wiki/3DES) (3DES) — симметричный блочный криптографический алгоритм, созданный на основе алгоритма DES с целью устранения главного недостатка последнего — малой длины ключа (56 бит), который может быть взломан методом перебора ключа.

В 3-DES был избран простой путь увеличения длины ключа без необходимости переходить на новый алгоритм — в нем над 64-битным блоком данных несколько раз производится шифрование алгоритмом DES (конечно, с разным ключом), в простейшем варианте это выглядит как: DES(k3;DES(k2;DES(k1;M))), где M - блок исходных данных, k1, k2 и k3 — ключи DES. Этот вариант известен как EEE — поскольку три операции DES являются шифрованием, более распространен вариант EDE (стандарт FIPS-46-3), в котором серединное шифрование DES с ключом k2 заменяется операцией расшифрования с тем же ключом (k2). В общем, длина ключа алгоритма 3-DES равна 168 битам (3x ключ DES)

В  2002  году  в  США  был  принят   стандарт  шифрования  взамен  старому  (DES).  Стандарт  носит  название  Advanced  Encryption  Standard  (AES).  В  отличие  от  отечественного,  избирался  на  конкурсной  основе.  В  данный  момент  является  одним  из  самых  распространенных  алгоритмов  симметричного  шифрования.

Алгоритм  AES  основан  на  архитектуре  “Square”,  что  в  переводе  означает  «Квадрат»,  которая  представляет  собой  прямые  преобразования  шифруемого  блока,  который  представлен  в  виде  двумерного  байтового  массива  размером  4х4.

За  один  раунд  шифруемый  блок  преобразуется  целиком,  таким  образом,  необходимую  сложность  преобразований  можно  получить  за  меньшее  число  раундов.

Каждый  раунд  заключается  в  сложении  по  модулю  два  начального  блока  данных  и  ключевого  элемента,  далее  следуют  три  операции,  рассмотренные  в  следующей  части.

В  алгоритме  AES  шифруемый  блок  представлен  в  виде  матрицы  4х4.  Все  операции  производятся  над  отдельными  байтами  матрицы,  а  так  же  над  ее  строками  и  столбцами.

В  каждом  раунде  происходят  следующие  преобразования:

­­- Операция  SubBytes  представляет  собой  замену  каждого  байта  массива  данных  новым  значением,  используя  таблицу  замены.  Такая  подстановка  обеспечивает  нелинейность  алгоритма  шифрования.

­- Операция  ShiftRows  выполняет  циклический  сдвиг  влево  всех  строк  массива  данных,  кроме  нулевой.  Шаг  смещения  байтов  зависит  от  номера  строки.

- Операция  MixColumns  выполняет  умножение  каждого  столбца  массива  данных,  которые  принимаются  за  многочлены  над  полем  GF(28),  на  фиксированный  полином.

https://sibac.info/sites/default/files/files/2015_05_26_StudTech/3_Bragina.files/image001.png.                                    (1)

умножение  по  модулю  https://sibac.info/sites/default/files/files/2015_05_26_StudTech/3_Bragina.files/image002.png.                                           (2)

Операция  AddRoundKey  выполняет  сложение  по  модулю  два  массива  данных  с  ключом.

В  алгоритме  шифрования  стандарта  AES  предусмотрено  10—14  раундов.  Но  достаточная  криптостойкость  алгоритма  достигается  уже  при  6—8  раундах.

В  стандарте  AES  расшифрование  происходит  путем  применения  обратных  операций  в  обратной  последовательности.  При  сопоставлении  алгоритмов  прямого  и  обратного  преобразований  можно  заметить,  что  они  практически  одинаковы,  за  исключением  того,  что  все  ключевые  моменты  выполняются  в  обратном  порядке.

В  стандарте  AES  ключ  для  каждого  раунда  вырабатывается  с  помощью  операции  расширения.  Длина  каждого  ключа  составляет  128,  192  или  256  бит.  Алгоритмы  определения  ключа  шифрования  различаются  незначительно.  Рассмотрим  на  примере  128-битного  ключа  или  четырех  4-байтовых  слов  wi,  wi+1,  wi+2,  wi+3.  Все  ключи  —  44-байтовых  слова.  Первые  четыре  слова  заполняются  ключом  шифра,  а  из  остальных  40  слов  выбираются  4  слова  для  ключа  раунда.  Слова  выбираются  следующим  образом:  четыре  первых  слова  являются  ключом  с  номером  0,  следующие  четыре  слова  —  ключом  для  первого  раунда  и  т.  д.

Формирование  последующих  раундовых  ключей  происходит  в  соответствии  с  формулами:

https://sibac.info/sites/default/files/files/2015_05_26_StudTech/3_Bragina.files/image003.png                                     (3)

https://sibac.info/sites/default/files/files/2015_05_26_StudTech/3_Bragina.files/image004.png  и  т.  д.                        (4)

 Изменение  первых  слов  в  каждом  ключе  раунда  происходит  по  следующей  формуле:

https://sibac.info/sites/default/files/files/2015_05_26_StudTech/3_Bragina.files/image005.png                                  (5)

Функция  g  выполняется  в  виде  последовательных  шагов:

1.  Rotword  —  сдвиг  влево  на  один  байт

2.  SubBytes  —  замена  каждого  байта

3.  Суммирование  по  модулю  два  байтов  с  раундовой  константой,  с  целью  избежания  симметрии  и  появления  слабых  ключей.

Несмотря  на  сложность  выбора  ключей  шифрования  в  AES,  метод  остается  достаточно  простым  и  эффективным.  В  данном  случае  атака  с  перебором  ключей  не  имеет  практического  значения.

**2. Стандарты шифрования Японии**

Рассмотрим такие наиболее известные алгоритмы шифрования, как MISTY1 и Camellia.

Алгоритм MISTY1 разработан в 1996 году японской компанией Mitsubishi Electric. Алгоритм имеет весьма интересную структуру – он основан на «вложенных» сетях. Алгоритм является сетью Фейстеля с различными четными и нечетными раундами. В нечетных раундах, по сравнению с четными, выполняется дополнительно операция FL, которая также выполняется и по завершении последнего раунда. Количество раундов строго не определено, но рекомендуется выполнять 8 раундов преобразований.   
Операция FL является достаточно простой: 32-битное входное значение разбивается на два субблока по 16 бит, над которыми выполняются операции сложения по модулю 2 и побитные логические операции «и» (&) и «или» (|), причем в логических операциях участвуют определенные фрагменты расширенного ключа шифрования для операции FL: KL1 и KL2 (см. ниже).  
Несравнимо более сложной является операция FO. Она и представляет собой «второй уровень» сети Фейстеля внутри основной структуры алгоритма. В данной операции 32-битное входное значение также делится на два 16-битных фрагмента, один из которых обрабатывается операцией сложения по модулю 2 с определенным фрагментом ключа для операции FO (KOx) и операцией FI, после чего значения субблоков складываются по модулю 2 и меняются местами. Фактически, схема является трехраундовой сетью Фейстеля с дополнительным сложением по модулю 2 после финального раунда.  
В отличие от операций FL и FO, операция FI обрабатывает 16-битные блоки входных данных. И снова это «вложенная» 3-раундовая сеть Фейстеля, обрабатывающая 7-битный и 9-битный субблоки, над которыми выполняются следующие операции:

1. Табличные замены S7 и S9 над 7- и 9-битным субблоком соответственно.
2. Сложение субблоков между собой по модулю 2, причем в первом и третьем раундах 7-битный субблок дополняется нулями и результатом сложения является 9-битный субблок, а во втором раунде при сложении отбрасываются два левых бита 9-битного субблока и результатом сложения является 7-битный субблок.
3. Сложение по модулю 2 соответствующих субблоков с 7- и 9-битным фрагментами расширенного ключа шифрования KI1 и KI2, выполняемое во втором раунде.

Размерность ключа алгоритма MISTY1 – 128 бит. Перед началом работы алгоритма или параллельно с описанными выше операциями выполняется процедура расширения ключа шифрования, в которой вычисляются фрагменты ключа, используемые в операциях FL, FO и FI. Процедура расширения ключа не является сложной, кроме того, в ней используется фрагмент самого алгоритма – функция FI, поэтому на расширение ключа шифрования не требуются дополнительные ресурсы (в отличие от многих других алгоритмов шифрования, в которых расширение ключа может быть достаточно ресурсоемкой операцией, – например, данный недостаток есть у алгоритма MARS – одного из финалистов конкурса AES).  
В результате исследований алгоритма MISTY1 эксперты не обнаружили каких-либо слабостей у данного алгоритма при достаточно высокой скорости шифрования, что также является немаловажной характеристикой криптоалгоритмов. Стоит сказать и о том, что вариант алгоритма MISTY1 – алгоритм KASUMI – в 2000 году стал стандартом шифрования мобильной связи W-CDMA.

Camellia - алгоритм симметричного блочного шифрования (размер блока 128 бит, ключ 128, 192, 256 бит), один из финалистов европейского конкурса NESSIE (наряду с AES и Shacal-2), разработка японских компаний Nippon Telegraph and Telephone Corporation и Mitsubishi Electric Corporation (представлен 10 марта 2000 г.). Сертифицирован японской организацией CRYPTREC как рекомендованный для промышленного и государственного использования алгоритм.

Camellia является дальнейшим развитием алгоритма шифрования E2, одного из алгоритмов, представленных на конкурсе AES и с использованием элементов алгоритма MISTY1.

Структура алгоритма основана на классической цепи Фейстеля с предварительным и финальным забеливанием. Цикловая функция использует нелинейное преобразование (S-блоки), блок линейного рассеивания каждые 16 циклов (побайтовая операция XOR) и байтовую перестановку.

В зависимости от длины ключа имеет 18 циклов (128 разрядный ключ), либо 24 цикла (192 и 256 разрядный ключ).

Поддержка алгоритма Camellia введена в 2008 году в браузере Mozilla Firefox 3, однако отключена в 2014 году в Mozilla Firefox. Позднее в том же году команда разработчиков FreeBSD объявила, что поддержка данного шифрования также была включена в FreeBSD 6.4-RELEASE. В сентябре 2009 года GNU Privacy Guard добавили поддержку Camellia в версии 1.4.10. Кроме того, многие популярные библиотеки безопасности, такие как Crypto++, GnuTLS, PolarSSL и OpenSSL. также включают в себя поддержку Camellia. Алгоритм патентован, однако распространяется под рядом свободных лицензий.

**Заключение**

Алгоритмы шифрования с использованием ключей предполагают, что данные не сможет прочитать никто, кто не обладает ключом для их расшифровки. Они могут быть разделены на два класса, в зависимости от того, какая методология криптосистем напрямую поддерживается ими.

#### Для шифрования и расшифровки используются одни и те же алгоритмы. Один и тот же секретный ключ используется для шифрования и расшифровки. Этот тип алгоритмов используется как симметричными, так и асимметричными криптосистемами.

Одной из наиболее известных криптографических систем США с закрытым ключом является DES. Эта система сегодня не обладает статусом государственного стандарта в области шифрования данных.

Вместе с этим можно отметить, что систему DES вполне можно использовать в небольших и средних приложениях для шифрования данных, имеющих небольшую ценность. Для шифрования данных государственной важности в настоящее время в США используется на блочный шифр, AES, в основу которого был положен шифр Rijndael, разработанный бельгийскими специалистами.

В работе также были рассмотрены такие стандарты шифрования, как алгоритм MISTY1 и алгоритм Camellia.

**Список использованной литературы**

1. Мелихова О.А., Чумичев В.С., Джамбинов С.В., Гайдуков А.Б. Некоторые аспекты криптографического взлома и повышения надежности алгоритмов шифрования// Молодой ученый. - Казань, № 11(91), 2015. - С. 392—394.
2. Мелихова О. А., Григораш А. С., Джамбинов С. В. [и др.] Сравнительный анализ современных алгоритмов шифрования // Инновации в науке: сб. ст. по матер. L междунар. науч.-практ. конф. № 10(47). – Новосибирск: СибАК, 2015.
3. Орлов В. Г., Мазуркевич Д. О. Алгоритмы шифрования в публичных беспроводных сетях // T-Comm. 2011. №10. URL: http://cyberleninka.ru/article/n/algoritmy-shifrovaniya-v-publichnyh-besprovodnyh-setyah (дата обращения: 05.12.2016).
4. Панасенко С.П. Алгоритмы шифрования:специальный справочник. СПб.: БВХ-Петербург, 2009. – 576 с.
5. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение - М.: СОЛОН-Пресс, 2004.
6. Чмора А.Л. Современная прикладная криптография. 2-е изд., стер. – М.: Гелиос АРВ, 2004. – 256с.: ил.