МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ОРЛОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

имени И.С. ТУРГЕНЕВА»

Ливенский филиал ОГУ им. И.С. Тургенева

Технико-экономический факультет

Кафедра информационных технологий и экономик

Творческая работа

На тему: «Криптография»

Выполнил студент 2-го курса

Группы ПО-22

Хорошилов Алексей

Руководитель

Шатохина Елена Николаевна

**1. Введение**

То, что информация имеет ценность, люди осознали очень давно - недаром переписка сильных мира сего издавна была объектом пристального внимания их недругов и друзей. Тогда-то и возникла задача защиты этой переписки от чрезмерно любопытных глаз. Древние пытались использовать для решения этой задачи самые разнообразные методы, и одним из них была тайнопись - умение составлять сообщения таким образом, чтобы его смысл был недоступен никому кроме посвященных в тайну. Есть свидетельства тому, что искусство тайнописи зародилось еще в доантичные времена. В наше время информация приобрела самостоятельную коммерческую ценность и стала широко распространенным, почти обычным товаром. Ее производят, хранят, транспортируют, продают и покупают, а значит - воруют и подделывают - и, следовательно, ее необходимо защищать. Широкое применение компьютерных технологий и постоянное увеличение объема информационных потоков вызывает постоянный рост интереса к криптографии. В последнее время увеличивается роль программных средств защиты информации, не требующих крупных финансовых затрат в сравнении с аппаратными криптосистемами. Современные методы шифрования гарантируют практически абсолютную защиту данных.

**2. Основные определения**

***Конфиденциальность***- невозможность получения информации из преобразованного массива без знания дополнительной информации (ключа).

***Аутентичность***информации состоит в подлинности авторстваи целостности.

***Криптоанализ***объединяет математические методы нарушения конфиденциальности и аутентичности информации без знания ключей.

Под ***шифром***понимается совокупность обратимых преобразований множества открытых данных на множество зашифрованных данных, заданных алгоритмом криптографического преобразования. В шифре всегда различают два элемента: алгоритм и ключ. Алгоритм позволяет использовать сравнительно короткий ключ для шифрования сколь угодно большого текста.

***Криптографическая система***, или ***шифр***представляет собой семейство преобразований открытого текста в шифрованный. Членам этого семейства можно взаимно однозначно сопоставить число ***k***, называемое ***ключом.***

***Ключ***- конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного варианта из совокупности всевозможных для данного алгоритма. Секретность ключа должна обеспечивать невозможность восстановления исходного текста по шифрованному.

Обычно ключ представляет собой последовательный ряд букв алфавита. Следует отличать понятия "ключ" и "пароль". ***Пароль***также является секретной последовательностью букв алфавита, однако используется не для шифрования (как ключ), а для аутентификации субъектов.

***Электронной (цифровой*) *подписью***называется присоединяемое к тексту его криптографическое преобразование, которое позволяет при получении текста другим пользователем проверить авторство и целостность сообщения.

***Зашифрованием***данных называется процесс преобразования открытых данных в зашифрованные с помощью шифра, а ***расшифрованием***данных - процесс преобразования закрытых данных в открытые с помощью шифра.

***Дешифрованием***называется процесс преобразования закрытых данных в открытые при неизвестном ключе и, возможно, неизвестном алгоритме, т.е. методами криптоанализа.

***Шифрованием***называется процесс зашифрования или расшифрования данных. Также термин шифрование используется как синоним зашифрования. Однако неверно в качестве синонима шифрования использовать термин "кодирование" (а вместо "шифра" - "код"), так как под кодированием обычно понимают представление информации в виде знаков (букв алфавита).

***Криптостойкостью***называется характеристика шифра, определяющая его стойкость к дешифрованию. Обычно эта характеристика определяется периодом времени, необходимым для дешифрования.

***Криптология*** - это наука о преобразовании информации для обеспечения ее секретности, состоящая из двух ветвей: криптографии и криптоанализа.

***Криптография*** - наука о способах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей. Исторически первой задачей криптографии была защита передаваемых текстовых сообщений от несанкционированного ознакомления с их содержанием, известного только отправителю и получателю, все методы шифрования являются лишь развитием этой философской идеи. С усложнением информационных взаимодействий в человеческом обществе возникли и продолжают возникать новые задачи по их защите, некоторые из них были решены в рамках криптографии, что потребовало развития новых подходов и методов.

**3. Шифры, их виды и свойства**

В криптографии криптографические системы (или шифры) классифицируются следующим образом:

-симметричные криптосистемы

-асимметричные криптосистемы

***3.1 Под симметричными криптографическими системами*** понимаются такие криптосистемы, в которых для шифрования и расшифрования используется один и тот же ключ, хранящийся в секрете. Все многообразие симметричных криптосистем основывается на следующих базовых классах:

*I. Моно - и многоалфавитные подстановки.*

Моноалфавитные подстановки - это наиболее простой вид преобразований, заключающийся в замене символов исходного текста на другие (того же алфавита) по более или менее сложному правилу. В случае моноалфавитных подстановок каждый символ исходного текста преобразуется в символ шифрованного текста по одному и тому же закону. При многоалфавитной подстановке закон преобразования меняется от символа к символу. Один и тот же шифр может рассматриваться и как моно - и как многоалфавитный в зависимости от определяемого алфавита.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Исходные символы шифруемого текста | а | б | в | г | д | е | ж | з | и | к | л | м | н | о | п | р | с | т | у | ь | … |
| Заменяющие символы | s | р | x | l | r | z | i | m | a | y | e | d | w | t | b | g | v | n | j | o | … |

Например, самой простой разновидностью является прямая (простая) замена, когда буквы шифруемого сообщения заменяются другими буквами того же самого или некоторого другого алфавита. Таблица замены может иметь следующий вид:

Используя эту таблицу, зашифруем слово двигатель. Получим следующее: rxflsnzeo

*II. Перестановки -*перестановка местами символов исходного текста по некоторому правилу. Шифры перестановок в настоящее время не используются в чистом виде, так как их криптостойкость недостаточна, но они входят в качестве элемента в очень многие современные криптосистемы.

Самая простая перестановка - написать исходный текст наоборот и одновременно разбить шифрограмму на пятерки букв. Например, из фразы

ПУСТЬ БУДЕТ ТАК, КАК МЫ ХОТЕЛИ

получится такой шифротекст:

ИЛЕТО ХЫМКА ККАТТ ЕДУБЪ ТСУП

*III. Блочные шифры -*семейство обратимых преобразований блоков (частей фиксированной длины) исходного текста. Фактически блочный шифр - это система подстановки на алфавите блоков. Она может быть моно - или многоалфавитной в зависимости от режимаблочного шифра. Иначе говоря, при блочном шифровании информация разбивается на блоки фиксированной длины и шифруется поблочно. Блочные шифры бывают двух основных видов: шифры перестановки (transposition, permutation, P-блоки) и шифры замены (подстановки, substitution, S-блоки) 1. В настоящее время блочные шифры наиболее распространены на практике.

Американский стандарт криптографического закрытия данных *DES (*Data Encryption Standard), принятый в 1978 г., является типичным представителем семейства блочных шифров и одним из наиболее распространенных криптографических стандартов на шифрование данных, применяемых в США. Этот шифр допускает эффективную аппаратную и программную реализацию, причем возможно достижение скоростей шифрования до нескольких мегабайт в секунду. Первоначально метод, лежащий в основе данного стандарта, был разработан фирмой IBMдля своих целей. Он был проверен Агентством Национальной Безопасности США, которое не обнаружило в нем статистических или математических изъянов.

*DES*имеет блоки по 64 бит и основан на 16-кратной перестановке данных, также для шифрования использует ключ в 56 бит. Существует несколько режимов *DES*: *Electronic Code Book (ECB*) и *Cipher Block Chaining(CBC*).56 бит - это 8 семибитовыхсимволов, т.е. пароль не может быть больше чем восемь букв. Если вдобавок использовать только буквы и цифры, то количество возможных вариантов будет существенно меньше максимально возможных 256. Однако, данный алгоритм, являясь первым опытом стандарта шифрования, имеет ряд недостатков. За время, прошедшее после создания *DES*, компьютерная техника развилась настолько быстро, что оказалось возможным осуществлять исчерпывающий перебор ключей и тем самым раскрывать шифр.

*IV. Гаммирование -*преобразование исходного текста, при котором символы исходного текста складываются с символами псевдослучайной последовательности (гамме), вырабатываемой по некоторому правилу. В качестве гаммы может быть использована любая последовательность случайных символов. Процедуру наложения гаммы на исходный текст можно осуществить двумя способами. При первом способе символы исходного текста и гаммы заменяются цифровыми эквивалентами, которые затем складываются по модулю *k*, где *k -*число символов в алфавите. При втором методе символы исходного текста и гаммы представляются в виде двоичного кода, затем соответствующие разряды складываются по модулю 2. Вместо сложения по модулю 2 при гаммировании можно использовать и другие логические операции.

Таким образом, симметричными криптографическими системами являются криптосистемы, в которых для шифрования и расшифрования используется один и тот же ключ. Достаточно эффективным средством повышения стойкости шифрования является комбинированное использование нескольких различных способов шифрования. Основным недостатком симметричного шифрования является то, что секретный ключ должен быть известен и отправителю, и получателю.

**3.2 Асимметричные криптографические системы**

Эти системы характеризуются тем, что для шифрования и для расшифрования используются разные ключи, связанные между собой некоторой зависимостью. Применение таких шифров стало возможным благодаря К. Шеннону, предложившему строить шифр таким способом, чтобы его раскрытие было эквивалентно решению математической задачи, требующей выполнения объемов вычислений, превосходящих возможности современных ЭВМ (например, операции с большими простыми числами и их произведениями). Один из ключей (например, ключ шифрования) может быть сделан общедоступным, и в этом случае проблема получения общего секретного ключа для связи отпадает. Если сделать общедоступным ключ расшифрования, то на базе полученной системы можно построить систему аутентификации передаваемых сообщений. Поскольку в большинстве случаев один ключ из пары делается общедоступным, такие системы получили также название криптосистем с открытым ключом. Первый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование данных с помощью известного ключа невозможно. Для расшифрования данных получатель зашифрованной информации использует второй ключ, который является секретным. Разумеется, ключ расшифрования не может быть определен из ключа зашифрования.

В настоящее время наиболее развитым методом криптографической защиты информации с известным ключом является *RSA*, названный так по начальным буквам фамилий его изобретателей (Rivest, Shamir и Adleman) и представляющий собой криптосистему, стойкость которой основана на сложности решения задачи разложения числа на простые сомножители. Простыми называются такие числа, которые не имеют делителей, кроме самих себя и единицы. А взаимно простыми называются числа, не имеющие общих делителей, кроме 1.

Криптосистема *RSA* широко применяется в Интернете. Когда пользователь подсоединяется к защищенному серверу, то здесь применяется шифрование открытым ключом с использованием идей алгоритма *RSA*. Криптостойкость *RSA* основывается на том предположении, что исключительно трудно, если вообще реально, определить закрытый ключ из открытого. Для этого требовалось решить задачу о существовании делителей огромного целого числа. До сих пор ее аналитическими методами никто не решил, и алгоритм *RSA* можно взломать лишь путем полного перебора.

Таким образом, асимметричные криптографические системы - это системы, в которых для шифрования и для расшифрования используются разные ключи. Один из ключей даже может быть сделан общедоступным. При этом расшифрование данных с помощью известного ключа невозможно.

**4. Заключение**

Криптография является одним из наиболее мощных средств обеспечения конфиденциальности и контроля целостности информации. Во многих отношениях она занимает центральное место среди программно-технических регуляторов безопасности. Например, для портативных компьютеров, физически защитить которые крайне трудно, только криптография позволяет гарантировать конфиденциальность информации даже в случае кражи.

**5. Список литературы**

1. Златопольский Д.М. Простейшие методы шифрования текста. /Д.М. Златопольский - М.: Чистые пруды, 2007
2. Молдовян А. Криптография. /А. Молдовян, Н.А. Молдовян, Б.Я. Советов - СПб: Лань, 2001
3. http://ru. wikipedia.org
4. http://cryptoblog.ru