ЦИКТ ЦЕНТР ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ГАПОУ КП № 11

«КОЛЛЕДЖ ПРЕДПРИНИМАТЕЛЬСТВА №11»

Криптография

Предисловие

Информация - это одна из самых ценных вещей в современной жизни. Появление глобальных компьютерных сетей сделало простым получение доступа к информации как для отдельных людей, так и для больших организаций. Но легкость и скорость доступа к данным с помощью компьютерных сетей, таких как Интернет, также сделали значительными следующие угрозы безопасности данных при отсутствии мер их защиты:

Неавторизованный доступ к информации

Неавторизованное изменение информации

Неавторизованный доступ к сетям и другим сервисам

Другие сетевые атаки, такие как повтор перехваченных ранее транзакций и атаки типа "отказ в обслуживании"

Определение

Криптография — наука о методах обеспечения конфиденциальности (невозможности прочтения информации посторонним), целостности данных (невозможности незаметного изменения информации), аутентификации (проверки подлинности авторства или иных свойств объекта), а также невозможности отказа от авторства.

История

Изначально криптография изучала методы шифрования информации — обратимого преобразования открытого (исходного) текста на основе секретного алгоритма или ключа в шифрованный текст (шифротекст). Традиционная криптография образует раздел симметричных криптосистем, в которых зашифрование и расшифрование проводится с использованием одного и того же секретного ключа. Помимо этого раздела современная криптография включает в себя асимметричные криптосистемы, системы электронной цифровой подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовую криптографию.

Отличия

Криптография не занимается защитой от обмана, подкупа или шантажа законных абонентов, кражи ключей и других угроз информации, возникающих в защищённых системах передачи данных.

Криптография — одна из старейших наук, её история насчитывает несколько тысяч лет.

Криптосистема

Криптосистема работает по определенной методологии (процедуре). Она состоит из : одного или более алгоритмов шифрования (математических формул); ключей, используемых этими алгоритмами шифрования; системы управления ключами; незашифрованного текста; и зашифрованного текста (шифртекста).

Согласно методологии сначала к тексту применяются алгоритм шифрования и ключ для получения из него шифртекста. Затем шифртекст передается к месту назначения, где тот же самый алгоритм используется для его расшифровки, чтобы получить снова текст. Также в методологию входят процедуры создания ключей и их распространения (не показанные на рисунке).

Алгоритмы шифрования

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.

Виды:

Симметричные алгоритмы

Асимметричные алгоритмы

Хэш-функции

Механизмы аутентификации

Электронные подписи и временные метки

Симметричные алгоритмы

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.

Типы:

DES

3-DES

FEAL

IDEA

Skipjack

CAST

Поточные шифры

Асимметричные алгоритмы

Асимметричные алгоритмы используются в асимметричных криптосистемах для шифрования симметричных сеансовых ключей (которые используются для шифрования самих данных).

Используется два разных ключа - один известен всем, а другой держится в тайне. Обычно для шифрования и расшифровки используется оба этих ключа. Но данные, зашифрованные одним ключом, можно расшифровать только с помощью другого ключа.

Типы:

RSA

ECC

Эль-Гамаль

Хэш-функции

Хэш-функции являются одним из важных элементов криптосистем на основе ключей. Их относительно легко вычислить, но почти невозможно расшифровать. Хэш-функция имеет исходные данные переменной длины и возвращает строку фиксированного размера (иногда называемую дайджестом сообщения - MD), обычно 128 бит. Хэш-функции используются для обнаружения модификации сообщения (то есть для электронной подписи).

Типы:

MD2

MD4

MD5

SHA

Механизмы аутентификации

Эти механизмы позволяют проверить подлинность личности участника взаимодействия безопасным и надежным способом.

Типы:

Пароли или PIN-коды

Одноразовый пароль

CHAP

Встречная проверка

Электронные подписи и временные

Электронная подпись позволяет проверять целостность данных, но не обеспечивает их конфиденциальность. Электронная подпись добавляется к сообщению и может шифроваться вместе с ним при необходимости сохранения данных в тайне. Добавление временных меток к электронной подписи позволяет обеспечить ограниченную форму контроля участников взаимодействия.

Типы:

DSA

RSA

MAC

DTS

Шифр цезаря

Шифр Цезаря, также известный как шифр сдвига, код Цезаря или сдвиг Цезаря — один из самых простых и наиболее широко известных методов шифрования. Шифр Цезаря — это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом вправо на 3, А была бы заменена на Г, Б станет Д, и так далее. Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами.

Шифр Цезаря

Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все ещё имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

История

Шифр Цезаря называют в честь Юлия Цезаря, который согласно «Жизни двенадцати цезарей» Светония использовал его со сдвигом 3, чтобы защищать военные сообщения.

Если кто-либо хотел дешифровать его и понять его значение, то он должен был подставлять четвертую букву алфавита, а именно, D, для A, и так далее, с другими буквами.

Его племянник, Август, также использовал этот шифр, но со сдвигом вправо на один, и он не повторялся к началу алфавита: Всякий раз, когда он записывал шифром, он записал B для A, C для B, и остальной части букв на том же самом принципе, используя AA для X.

Сообщение	К	Р	И	П	Т	О	Г	Р	А	Ф	И	Я
Номер 1	12	18	10	17	20	16	4	18	1	22	10	33
Номер 1 +5	17	23	15	22	25	21	9	23	6	27	15	5
Шифр	П	Х	Н	Ф	Ч	У	З	Х	Е	Щ	Н	Д

Пример

Шифрование с использованием ключа . Буква «Е» «сдвигается» на три буквы вперёд и становится буквой «З». Твёрдый знак, перемещённый на три буквы вперёд, становится буквой «Э», буква «Я», перемещённая на три буквы вперёд, становится буквой «В», и так далее. :

Исходный алфавит: АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
Шифрованный: ГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯАБВ

Оригинальный текст:

Съешь же ещё этих мягких французских булок, да выпей чаю.

Шифрованный текст получается путём замены каждой буквы оригинального текста соответствующей буквой шифрованного алфавита:

Фэзыя йз зьи ахлш пвёнлш чугрщцкфнлш дцосн, жг еютзм ъгб.

Base 16

Base 16 - это система счисления по основанию 16, т.е шестнадцатиричная система счисления. С ней вы могли и должны были столкнуться на уроках информатики. Алфавит этой кодировки состоит из цифр (0-9) и букв (A-F). Алгоритм преобразования остается примерно тем же, разве что теперь нам надо исходные двоичные числа разделить на тетрады (группы по 4 бита) и перевести их в соотвествии с таблицой кодировки в символы ASCII.

Base32

Base 32 использует 32 символа: A-Z (или a-z), 2-7. Может содержать в конце кодированной последовательности несколько спецсимволов (по аналогии с base64). В данном алгоритме преобразования нам необходимо будет разделять двоичные значения на группы по 5 бит.

Base32

Использует только 32 символа: A-Z (или a-z), 2-7. Может содержать в конце кодированной последовательности несколько спецсимволов (по аналогии с base64).

Преимущества: Последовательность любых байтов переводит в печатные символы. Регистронезависимая кодировка. Не используются цифры, слишком похожие на буквы (например, 0 похож на O, 1 на l).

Недостатки: Кодированные данные составляют 160% от исходных.

Base64

Позволяет кодировать информацию, представленную набором байтов, используя всего 64 символа: A-Z, a-z, 0-9, /, +. В конце кодированной последовательности может содержаться несколько спецсимволов (обычно “=”).

Преимущества: Позволяет представить последовательность любых байтов в печатных символах. В сравнении с другими Base-кодировками дает результат, который составляет только 133.(3)% от длины исходных данных.

Недостатки: Регистрозависимая кодировка.

Кодирование Base

В основном вам будет попадаться base 64. Его легко определить, т.к. на конце будет знак "=". Например, мы кодировали строку «АБВГД» в base 64 и у нас получился результат «wMHCw8Q=». Как мы видим, здесь присутсвует знак "=", который говорит нам о том, что строка зашифрована в base 64.

Base 16, 32, 64 легко декодировать онлайн-сервисами. Процесс кодирования почти ничем не отличается, разве, что вам нужно вбить в запросе не "decode", а "encrypt". Бывает, что нужно обращать внимание на то, какой кодировкой вы пользуетесь. В русскоязычной версии ОС "Windows" обычно используется кодировка windows-1251

Примеры алгоритмов шифрования

Hex

Пример строки

3132333a3b666c6167

Особенности В hex могут присутствовать только цифры 1234567890 и буквы abcdef. Длина строки должна быть четной.

Примеры алгоритмов шифрования

Base64

Пример строки

MTIzOjtmbGFnMQ==

Особенности На конце строки могут присутствовать от 0 до 2 знаков ==. Так же в строке могут быть прописные (заглавные) буквы и символы / и +.

Примеры алгоритмов шифрования

Ceasar cipher

Пример строки

pbhagrefvgr.bet

Особенности Кодируются только буквы (одного алфавита). По-умолчанию поворот на 13 (ROT13), но может быть и другим.

Примеры алгоритмов шифрования

Base32

Пример строки

GEYTCMJRGE======

Особенности Все буквы одного типа (например строчные). На конце от 0 до 6 знаков =

Примеры алгоритмов шифрования

Atom128

Пример строки

SfQ50x97+IctQfT2QfPm0x99+/CC

Особенности В середине строки могут присутствовать следующие символы: + / =

Примеры алгоритмов шифрования

URI encode

Пример строки

1234%27%22%D0%BF%D1%80%D0%B8%D0%B2%D0%B5%D1%82

Особенности Преобразуются все символы, кроме 1234567890 и abcdefghjklmnopqrstuvwxyz В некоторых случаях не используются =, а / и + заменены соответственно на * и -

Примеры алгоритмов шифрования

Demical

Пример строки

flag

Особенности Преобразуются абсолютно все символы.

Примеры алгоритмов шифрования

Morse

Пример строки

.---- ..--- ...-- ....-

Особенности Вместо . и - могут использоваться другие символы.

Примеры алгоритмов шифрования

Hackerize XS

Пример строки

1234Λß↻Đ☰∮ç╫¿├↑ღ∏□þ¶ ┏§⊥üƴ₪✕¥ᶾпривет

Особенности Заменяются только буквы английского алфавита.

Примеры алгоритмов шифрования

Reverse=

Пример строки

54321dlrowolleh

Особенности Чтение строки с конца.

Примеры алгоритмов шифрования

Binary

Пример строки

01101000 01100101 01101100 01101100 01101111

Особенности Пробелы могут быть не расставлены. Тогда длина строки будет делиться на 8, на 7 или на 6 (зависит от случая).

Примеры алгоритмов шифрования

Encool 2

Пример строки

1234 ¶ øød1øß ❣ привет

Особенности Кодируются только символы английского алфавита.

Примеры алгоритмов шифрования

MEGAN-35

Пример строки

RdNtSLX1lLranwDslLbrRZRuSdixTI/q

Особенности Аналогично Atom128.

Примеры алгоритмов шифрования

TRIPO-5

Пример строки

mYGKnj=znKAMmgTT

Особенности Аналогично Atom128

Примеры алгоритмов шифрования

GILA7

Пример строки

Bg=dCTzrCd/hB7GG

Особенности Аналогично Atom128.

Примеры алгоритмов шифрования

HAZZ-15

Пример

+gidJ4zoJdQL+H55

Особенности Аналогично Atom128.

Примеры алгоритмов шифрования

ESAB-46

Пример

vz5jND0mNjQpvA//

Особенности В строке могут присутствовать символы / и =

Примеры алгоритмов шифрования

TIGO-3FX

Пример

w1V3Dx+ID35TwFXX

Особенности Аналогично Atom128.

Примеры алгоритмов шифрования

FERON-74

Пример

WrSZdY6mdZwoW744

Особенности Аналогично Atom128.

Примеры алгоритмов шифрования

ZONG22

Пример

Xd0F19xc1FHMXZ22

Особенности Аналогично Atom128.