2 слайд

Симметричное шифрование - способ шифрования, в котором для шифрования и расшифрования применяется один и тот же ключ.

Простая перестановка без ключа — один из самых простых методов шифрования.

Происходит это всё следующим образом:

1. Есть данные, которые нужно зашифровать.

2. Есть ключ шифрования. С его помощью данные шифруются по какому-то алгоритму.

3. Тот, кто обладает ключом и знает алгоритм, может расшифровать сообщение.

4. Если не знать ключа, то расшифровать данные почти невозможно.

Aлгоритмы шифрования данных широко применяются в компьютерной технике в системах сокрытия конфиденциальной и коммерческой информации от злонамеренного использования сторонними лицами.

Главным принципом в них является условие, что передатчик и приемник заранее знают алгоритм шифрования, а также ключ к сообщению, без которых информация представляет собой всего лишь набор символов, не имеющих смысла.

Например, мессенджеры защищают с помощью таких шифров переписку (при этом ключ для симметричного шифрования обычно доставляется в асимметрично зашифрованном виде).

Симметричное шифрование используется для обмена данными во многих современных сервисах, часто в сочетании с асимметричным шифрованием.

-----------------------------------------

3 слайд

Классическими примерами симметричного алгоритма являются:

1)Простая перестановка

2)Одиночная перестановка по ключу

3)Двойная перестановка

4)Перестановка «Магический квадрат»

2)Более практический метод шифрования, называемый одиночной перестановкой по ключу, очень похож на предыдущий. Он отличается лишь тем, что колонки таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

(Например, Мы берем рандомное слово, и просто его символы меняем местами, вместе со столбцами)

3)Двойная перестановка используется для дополнительной скрытности, где можно повторно зашифровать сообщение, которое уже было зашифровано.

(Например, зашифровать сообщение по столбцам, а потом по строкам.)

4)Берем рандомный магический квадрат - это наш ключ(размера 4 \* 4) и по порядковым номерам записываем свое сообщение. Человек, который впервые увидит ваше сообщение ничего не поймет.

Также чем больше магический квадрат вы возьмете, тем сложнее, что ваш сообщение прочтут.

-----------------------------------------

4 слайд

Блочные шифры

\*AES— американский стандарт шифрования

\*DES — стандарт шифрования данных

в США

\*3DES (Triple-DES, тройной DES)

\*RC2 (Rivest Cipher или Ron’s Cipher)

\*RC5

\*Blowfish

\*Twofish

\*NUSH

\*IDEA (International Data Encryption

Algorithm)

И т.д.

Потоковые шифры

\*RC4(Алгоритм шифрования с ключом переменной длины)

\*SEAL (Software Efficient Algorithm, программно-эффективный алгоритм)

\*WAKE (World Auto Key Encryption algorithm, алгоритм шифрования на автоматическом ключе)

-----------------------------------------

5 слайд

Основное различие между блочным шифром и потоковым шифром заключается в том, что блочный шифр преобразует обычный текст в зашифрованный текст, принимая блок обычного текста за раз.

В то время как поточный шифр преобразует обычный текст в зашифрованный текст, принимая 1 байт обычного текста за раз.



-----------------------------------------

6 слайд

DES (Data Encryption Standard) — симметричный алгоритм шифрования, в котором один ключ используется как для шифрования, так и для расшифрования данных. Был разработан фирмой IBM в качестве официального стандарта.

DES имеет блоки по 64 бит и осуществляет 16 раундов с одним и тем же

набором операций(называемой цикловой структурой сети Фейстеля), для шифрования использует ключ с длиной 56 бит(в преобразовании учавствуют раундовые ключи по 48 бит - ключи, которые по разному шифруют твой текст(в зависимости от стандарта шифрования)).

Работает следующим образом:

\*Производит начальную перестановку (IP)

\*Расщепляет блок на левую и правую

половины;

\*Осуществляет 16 раундов с одним и тем же

набором операций

\*Соединяет половины блока

\*Производит конечную перестановку.

-----------------------------------------

7 слайд

3DES (Triple DES) был создан на основе алгоритма DES для устранения главного недостатка: небольшой длины ключа (56 бит), который можно взломать методом грубой силы.

Алгоритм 3DES используется в ситуациях, когда надежность алгоритма DES считается недостаточной. Чаще всего используется вариант шифрования на трех ключах

(Des-EDE3):

\*Открытый текст шифруется на первом ключе;

\*Полученный шифр-текст – на втором;

\*И наконец данные, полученные после второго шага, шифруются на третьем ключе.

Все три ключа выбираются независимо друг от друга.

Этот криптоалгоритм достаточно стоек ко всем атакам, но скорость в три раза ниже.

-----------------------------------------

8 слайд

AES (расширенный стандарт шифрования). Этот алгоритм шифрования с размером блока 128 бит и ключом 128/192/256 бит.

AES Используется различными программами сжатия файлов включая 7 Zip, WinZip и RAR

Сегодня библиотеки AES созданы для множества языков программирования, включая C, C ++, Java, Javascript и Python.

AES - жизненно важный инструмент в шифрование базы данных и VPN системы.

Алгоритм AES состоит из определенного количества раундов (от 10 до 14 – это зависит от размера блока и длины ключа) и выполняет четыре преобразования:

1) BS (ByteSub), 2) SR (ShiftRow),

3) МС (MixColumn), 4) АК (AddRoundKey)

-----------------------------------------

9 слайд

\* BS (ByteSub) – табличная замена каждого байта массива.

Преобразование BS является нелинейной байтовой подстановкой которая воздействует независимо на каждый байт массива, используя таблицу замен (подстановок) S-box;

\* SR (ShiftRow) – сдвиг строк массива. При этой операции первая строка остается без изменений, а остальные циклически побайтно сдвигаются влево на фиксированное число байтов, зависящее от размера массива.

\* МС (MixColumn) – операция над независимыми столбцами массива – каждый столбец по определенному правилу умножается на фиксированную матрицу с(х);

\* АК (AddRoundKey) – добавление ключа. Каждый бит массива складывается по модулю 2 с соответствующим битом ключа раунда(т.е производит сложение XOR - исключающее или), который, в свою очередь, определенным образом вычисляется из ключа шифрования.

-----------------------------------------

10 слайд

Расшифрование выполняется с помощью следующих обратных операций:

1. Табличная замена ByteSub обращается применением другой таблицы, которая является инверсной относительно таблицы, используемой при зашифровании.

2. Обратной операцией к ShiftRow является циклический сдвиг строк вправо.

3. Обратная операция для MixColumn– умножение по тем же правилам на другую матрицу d(x), удовлетворяющую условию

с(х) \* d(x) = 1.

4. Добавление ключа AddRoundKey является обратным самому себе, поскольку в нем используется только операция XOR(исключающее или(хотя бы одно true, но не оба сразу )).

Эти операции применяются при расшифровании в последовательности, обратной той, что использовалась при зашифровании.

-----------------------------------------

11 слайд

RC4 — потоковый шифр, широко применяющийся в различных системах защиты информации в компьютерных сетях (например, в протоколах SSL и TLS, алгоритмах обеспечения безопасности беспроводных сетей WEP и WPA).

Ядро алгоритма поточных шифров состоит из функции — генератора псевдослучайных битов (гаммы), который выдаёт поток битов ключа.

Алгоритм шифрования.

Функция генерирует последовательность битов(ki).

Затем последовательность битов посредством операции «суммирование по модулю два» (xor) объединяется с открытым текстом. (mi)

Расшифрование происходит в обратном порядке.

-----------------------------------------

12 слайд

У симметричного шифрования много преимуществ, но есть существенный недостаток – оно передает ключ. Чтобы избавится от этого недостатка(или снизить риск) нужно, чтобы передатчик и приемник заранее знали алгоритм шифрования, а также ключ к сообщению и не разглашали его.

Блочные шифры обладают большими преимуществами, чем поточные.

AES В настоящее время он считается одним из самых эффективных и безопасных симметричных шифров и поэтому широко используется.