Артемьева

**Системы биометрической аутентификации**

Простая перестановка:

В\_лесу\_родилась\_ель *(исход)*

Влесуродиласьель *(убираем пробелы)*

|  |  |  |  |
| --- | --- | --- | --- |
| В | У | И | Ь |
| Л | Р | Л | У |
| Е | О | А | Л |
| С | Д | с | Ь |

(Просто пишем по столбцам фразу)

Вуиь лрлу еоал сдсь *(зашифрованное)*

По ключу:

Используем ключ «ключ»

В\_лесу\_родилась\_ель *(исход)*

|  |  |  |  |
| --- | --- | --- | --- |
| К | Л | Ю | ч |
| 1 | 2 | 4 | 3 |
| В | У | И | Ь |
| Л | Р | Л | У |
| Е | О | А | Л |
| С | Д | с | Ь |

*(Нумеруем столбцы по алфавиту ключа)*

Вуьи лрул еола сдьс (*Зашифрованное по ключу. Ключ де-факто просто нужен для того, чтобы было видно в каком порядке нужно поставить столбцы)*

Магический квадрат:

Магический квадрат – квадрат, у которого сумма столбца/строки/диагонали будет одинакова.

Например:

1 15 14 4  
12 6 7 9  
 8 10 11 5  
13 3 2 16  
(Сумма любой будет 34)

Как шифровать с помощью данной милой формы буллинга интеллекта:

ПриезжаюСегодня (исход)

По порядку пихаем это в квадрат:

|  |  |  |  |
| --- | --- | --- | --- |
| 1 п | 15 я | 14 н | 4 е |
| 12 о | 6 ж | 7 а | 9 с |
| 8 ю | 10 е | 11 г | 5 з |
| 13 д | 3 и | 2 р | 16 |

Пяне ожас юегз дир- (зашифрованное)

**Это взято из задач. Херня полнейшая, но мб поможет кому**

**(Если нужно прочитать – растяните)**

Тема занятия: Криптографические методы защиты информации (слайды 1-16)

Ознакомиться с презентацией. Дать ответы на следующие вопросы

1. Дать определение понятиям: «Криптография», «Криптоанализ»

*Криптография* – наука (искусство) о защите информации от прочтения ее посторонними, о методах преобразования (шифрования) информации с целью ее защиты от незаконных пользователей.

*Криптоанализ* – наука о методах и способах вскрытия шифров и кодов, анализа надежности криптоалгоритмов.

1. Какие термины используют в криптографии? Дать описание и привести примеры

*Перестановка* – нарушение нормального порядка следования единиц информации, например, букв (СЕКРЕТ – ЕТКРСЕ).

Замена на основе *шифралфавита* – перечень эквивалентов, используемых для преобразования открытого текста в шифрованный. Иногда шифралфавит предусматривает несколько замен одного знака. Например, С {16, 21, 35, 72}, т. е. С заменяется одним из чисел. Этот выбор называется гомофоном. Время от времени в шифралфавит включают символ, который ничего не значит (символ-пустышка).

*Код* – огромный шифр замены. С одной стороны – тысячи слов, фраз, букв и слогов открытого текста, с другой – заменяющие их кодовые слова или кодовые обозначения.

*Шифр* – код, основной единицей которого является знак, несколько знаков или битовый блок.

*Криптограмма* – окончательно обработанное и отосланное сообщение.

Расшифровка (раскодирование) – преобразование шифротекста (кодотекста), при наличии ключа и системы шифрования.

*Стойкость шифра* – это сложность задачи его вскрытия.

*Сложность задачи* – минимальная сложность алгоритмов ее решения.

1. Дать определение понятию «Симметричные системы шифрования»

Симметричные системы шифрования – это системы шифрования, которые используют один и тот же ключ как на этапе зашифрования данных, так и на этапе их расшифрования.

1. **Охарактеризовать Простую перестановку. Зашифровать фразу «Накрыться медным тазом» без пробелов**

Простая перестановка без ключа — один из самых простых методов шифрования. Сообщение записывается в таблицу по столбцам. После того, как открытый текст записан колонками, для образования шифровки он считывается по строкам. Для использования этого шифра отправителю и получателю нужно договориться об общем ключе в виде размера таблицы.

//

НакрытьсяМеднымТазом

(теперь пишем в таблицу)

Нрсеыам

Аыядмз

Ктмнто

(Теперь пишем итог)

Нрсеыам аыядмз ктмнто

//

1. **Охарактеризовать Одиночную перестановку по ключу. Зашифровать фразу «Накрыться медным тазом» без пробелов. Ключ: ДЮШЕС**

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.

//

НакрытсяМеднымТазом (дюшес)

(под ключом, пишем такую же таблицу что и в предыдущем)

Дюшес

Ныдыз

Атемо

Ксдтм

Ряна

(выставляем номера под столбдами согласно алфавиту)

Дюшес

Ныдыз

Атемо

Ксдтм

Ряна

15423

(Теперь пишем согласно номерам)

Нызды амоет ктмдс раня

//

1. Охарактеризовать Двойную перестановку по ключу

Двойная перестановка по ключу – когда зашифрованное слово, шифрую заново другим словом, с другим ключом и другим размером слова.

1. **Охарактеризовать Перестановку «Магический квадрат Дюрера». Зашифровать фразу «Привести пример.». Числа для магического квадрата взять из презентации.**

Шифровка с помощью данного метода – пишешь слово по номерам (в нужном порядке) а после этого нужно по строкам записать слова.

//

ПривестиПример (исход)

16 3 2 13

5 10 11 8

9 6 8 12

4 15 14 1

(Берём вышеуказанный квадрат)

-ирр

еими

псте

в—п

(записываем итог)

-ирр еими псте в- -п

//

**Шифровка псевдослучайным**

1.1) пишем алфавит в строку (и другие символы).

1.2) присваиваем им числа по порядку

2) создаём случайный ключ

3) пишем строку: ключ + исходник (числовой) div кол-во символов

4) переводим получившуюся последовательность в символы.

**Идентификация** — это процедура распознавания субъекта по его идентификатору (проще говоря, это определение имени, логина или номера).

*Идентификация выполняется при попытке войти в какую-либо систему (например, в операционную систему или в сервис электронной почты).*

Идентификатором может быть:

* номер телефона
* номер паспорта
* e-mail
* номер страницы в социальной сети и т.д.

После идентификации производится аутентификация.

**Аутентификация** — это основа безопасности любой системы, которая заключается в проверке подлинности данных о пользователе сервером.

Примером аутентификации может быть сравнение пароля, введенного пользователем, с паролем, который сохранен в базе данных сервера. Подобная проверка может быть, как односторонней, так и взаимной — все зависит от способа защиты и политики безопасности сервиса.

Чтобы определить чью-то подлинность, можно воспользоваться тремя факторами:

1. **Пароль** – то, что мы знаем (слово, PIN-код, код для замка, графический ключ)
2. **Устройство** – то, что мы имеем (пластиковая карта, ключ от замка, USB-ключ)
3. **Биометрика** – то, что является частью нас (отпечаток пальца, портрет, сетчатка глаза)

Получается, что каждый раз, когда вы вставляете ключ в замок, вводите пароль или прикладываете палец к сенсору отпечатков пальцев, вы **проходите аутентификацию**.

Когда определили ID, проверили подлинность, уже можно предоставить и доступ, то есть, выполнить авторизацию.

**Авторизация** - это проверка, осуществляемая компьютерной системой или сайтом для идентификации пользователя перед получением им права доступа к системе или Интернет-ресурсу. Другими словами, это предоставление доступа к какому-либо ресурсу (например, к электронной почте).

Тема: **Функции хеширования и целостность данных**

**Сделать конспект, отвечая на вопросы. (слайд 1-15)**

1. Как переводится с английского языка слова: hash, hashing

Путаница или мешанина. Hashing = рубить, крошить, спутывать

1. Что позволяла сделать хэш-функция?

Привести любой массив данных к числу заданной длинны

1. Дать определение понятию «хэширование»

Преобразование входного массива данных произвольной длинны, в выходную строку фиксированной длинны

1. Привести пример где и как используется хэширование

Проверка целостности при передачи пакетов по протоколу TCP/IP (и ряду других),

1. Дать определение понятию «хэш-функция»

Функция, преобразующая исходное сообщение в сообщение фиксированной длинны   
(прообраз -> хеш-образ)

1. Привести пример того, где используются хэш-функции

Блокчейн, криптография

1. Дать определение понятию «коллизия хеш-функции»

Ситуация, при которой разные файлы имеют одинаковый хеш-код (возможно если длинна хеш-кода маленькая)

1. Какими свойствами должна обладать хеш-функция?

* функция должна уметь приводить любой объем данных к числу заданной длины (по сути это сжатие до битовой последовательности заданной длины особым способом)
* малейшее изменение (хоть на один бит) входных данных должно приводить к полному изменению хеша
* должна быть стойкой в обратной операции, т.е. вероятность восстановления исходных данных по хешу должна быть весьма низкой
* должна иметь как можно более низкую вероятность возникновения коллизий
* хорошая хеш-функция не должна сильно нагружать ПК при своем исполнении. От этого сильно зависит скорость работы системы на ней построенной
* алгоритм работы функции должен быть открытым, чтобы любой желающий мог бы оценить ее криптостойкость, т.е. вероятность восстановления начальных данных по выдаваемому хешу

1. Описать популярные хеш-алгоритмы сжатия: CRC32, MD5, SHA-1, ГОСТ Р 34.11-2012

CRC32 — используется именно для создания контрольных сумм. Есть много вариаций этого алгоритма (число после CRC означает длину получаемого хеша в битах), в зависимости от нужной длины получаемого хеша. Функция очень простая и нересурсоемкая. В связи с этим используется для проверки целостности пакетов в различных протоколах передачи данных.

MD5 — старая, но до сих пор очень популярная версия уже криптографического алгоритма, которая создает хеш длиной в 128 бит. Хотя стойкость этой версии на сегодняшний день и не очень высока, она все равно часто используется как еще один вариант контрольной суммы, например, при скачивании файлов из сети.

SHA-1 — криптографическая функция формирующая хеш-суммы длиной в 160 байт. Сейчас идет активная миграция в сторону SHA-2, которая обладает более высокой устойчивостью, но SHA-1 по-прежнему активно используется хотя бы в качестве контрольных сумм. Но она так же по-прежнему используется и для хранения хешей паролей в базе данных сайта.

ГОСТ Р 34.11-2012 — текущий российский криптографический алгоритм введенный в работу в 2013 году (ранее использовался ГОСТ Р 34.11-94). Длина выходного хеша может быть 256 или 512 бит. Обладает высокой криптостойкостью и довольно хорошей скоростью работы. Используется для электронных цифровых подписей в системе государственного и другого документооборота.