Защита информации криптография

Носов В.А.

Механико-математический факультет МГУ

Область применения

- Защите подлежат все виды ценной информации.

- Стержнем этой науки является КРИПТОГРАФИЯ

Что такое криптография

Это наука о способах и средствах изменения передаваемого сообщения с целью сделать его непонятным для непосвященных лиц.

Возраст криптографии

Криптография существует с момента появления письменности-систем графики, алфавита и орфографии языков.

Социология криптографии

- До 80-х годов XX-го века- криптографией занимались только госучреждения, отвечающие за информационную безопасность.
- С 80-х криптографией занимаются также гражданские и общественные организации. Криптография становится массовой наукой.

Классики математики-криптографы

- Аристотель(384-322 до н.э.)
- Кардано Д.(1501-1576)
- Виет Ф.(1540-1603)
- Валлис Д.(1616-1703)
- Эйлер Л.(1707-1783)

Математики нового времени

- Шеннон К.(теория информации)
- Котельников В.А.(теория информации)
- Колмогоров А.Н.(теория вероятностей)
- Марков А.А.(теория алгоритмов)
- Гельфонд А.О.(теория чисел)

Законодательные акты РФ

- Доктрина информационной безопасности
- Об информации, информатизации и защите информации
- О связи
- О государственной тайне
- О цифровой подписи
- О безопасности

Образовательные стандарты

- 075100 криптография
- 075200 компьютерная безопасность
- 075300 организация и технология защиты информации
- 075400 комплексная защита объектов информатизации
- 075500 комплексное обеспечение информационной безопасности автоматизированных систем

Специализации МГУ

- Математические методы информационной безопасности

(механико-математический факультет)

- Программные методы информационной безопасности

(факультет вычислительной математики и кибернетики)

Периоды развития криптографии

-Криптография как искусство
(Древние и средние века)
-Криптография как ремесло
(17-19 вв)
-Криптография как наука
(20-й век)
- Криптография как вторая грамотность
(21-й век)

Современная криптография

Характеризуется

- Сложным подходом и классификацией задач по классам сложности.
- Числовым кодированием и числовыми алгоритмами преобразований данных.

Новые понятия криптографии

- Односторонняя функция и
  односторонняя функция с секретом
- Хэш-функция и
  параметрическая хэш-функция
- Протоколы выработки и распределения ключей

Классические шифры

- Простая и сложная замена букв
- Замена по латинскому квадрату
- Решетка Кардано
- Квадрат Полибия
- Значковые шифры

Классические системы второй мировой войны

- Германия- Энигма
- США-Машина Хагелин
- СССР-Машина К-37

Современные стандарты шифрования

- DES
- IDEA
- Гост 28147-89
- RSA

Стандарты цифровой подписи

- DSS- стандарт США
- Гост Р 34 10-94 Россия
- Стандарт RSA

Финансовая криптография

- Система Pay Word
- Система MicroMint
- Электронные деньги Яндекс

Классическая математика в криптографии

- Математическая логика и теория алгоритмов(криптографические протоколы, сложность алгоритмов)
- Теория чисел (дискретное логарифмирование, факторизация чисел)
- Теория вероятностей (вероятностные алгоритмы, датчики случайных чисел)

Дискретная математика в криптографии

- Алгебра (группы подстановок, теория конечных полей, булева алгебра)
- Дискретная математика (Дискретные функции и отображения. Теория автоматов. Комбинаторные структуры:

Латинские прямоугольники, блок-схемы, конечные проективные плоскости, рекурренты.

Новые применения криптографии

- 1 Цифровая подпись документа
- 2 Аутентификация пользователя
- 3 Целостность документа
- 4 Конфиденциальность сообщения

Переход к цифровым технологиям

- Код ASCII-American Standard Cod for Information Interchange
- Пример TO BE OR NOT TO BE

(быть или не быть- Гамлет)

84793266693279823278898 4

328479326669

Применение больших чисел

- Секунд в году---- 3.10 exp7
- Тактов ЭВМ в год- 1,6. 10 exp15
- Бинарных строк дл. 64 3,4. 10 exp 19
- Бинарных строк дл. 128 3,4 .10 exp 38
- Бинарных строк дл. 256 1,2. 10 exp 77
- Простых чисел 75-разрядов

  5,2. 10 exp72

Шифр Цезаря

- Замена букв текста на буквы, отстоящие на три позиции в алфавите.
- Пример VENI, VIDI, VICI

(пришел, увидел, победил)

YHQL YLGL YLFL

Послание Ю. Цезаря сенату о победе в понтийской войне

Тарабарская грамота

- Замена согласных букв алфавита на симметричные буквы относительно середины.
- Пример Рыба с головы гниет
- МЫЩАЛЧОСОШЫЧПИЕК

Шифрование в стандарте RSA

- Пример 1) Выбираем простые числа

p и q (7 и 11). Тогда N=p.q=77.

2) Выбираем к1=17 и к2=33

3) Шифруются буквы из интервала 1,2,…,76. (вычеты по модулю 77)

4) Шифрование на к1 x -> xexp17.

5) Расшифрование на к2 y –> yexp33.

Подпись в стандарте RSA

- По документу M вычисляется значение

Хэш-функции H(M)=m и подпись S есть число mexp(D), где D-секретный ключ. Проверка подписи- нахождение числа

m1=Sexp(E)-где E-открытый ключ и сравнение чисел м и м1.

Документальный фильм ОРТ об истории и значении криптографии

Межрегиональная олимпиада
по криптографии
http://v-olymp.ru
www.olimpiada.ru
www.academy.fsb.ru
8-985-137-35-93

КРАТКИЕ ВЫВОДЫ

Защита информации есть важнейшая задача в век информационных технологий.

Знание ее основ равносильно владению грамотности.

Спасибо за внимание!

Контактная информация-

www.vnosov40.mail.ru