План курса ЗЭШ «Основные понятия криптографии»

Речистов Григорий

21 декабря 2008 г.

1 Введение.

Защита информации. Криптография как одна из важных, но не единственных составляющих принципов ЗИ. История развития. Шифрование древних времён, периода второй мировой войны. Базовые понятия: открытый текст, шифрограмма, ключ, канал передачи данных, процессы зашифрования, дешифрования, расшифрования, отличия между ними. Алиса, Боб, Кэрол... Пример простейшего алгоритма – шифр Цезаря. Атака на шифр Цезаря – частотный анализ.

2 Задачи сторон.

Задачи криптографа: безопасность данных, аутентификация, идентификация сторон, подтверждение целостности сообщения. Задачи криптоаналитика: восстановление открытого текста по доступным парам «открытый текст» – «шифрограмма», восстановление ключа, подделка сообщений. Основной принцип криптографии: стойкость методики шифрования не должна определяться скрытностью алгоритма, а определяется только параметрами и неизвестностью ключа.

3 Некоторые математические основания используемых в криптографии алгоримтов.

Понятие алгоритмической сложности алгоритмов. Кратко о задачах класса P, NP-сложные, NP-полные. Эквивалентность классов, страшная диаграмма вложенности. Классификация алгоритмов по стойкости ко взлому: абсолютно стойкие (единственный пример – одноразовый блокнот), условно стойкие, нестойкие. Математические задачи, применяемые в криптографии: Однонаправленные функции Разложение числа на множители Укладка рюкзака Вычисления в поле Галуа. Генерация простых чисел и проверка чисел на простоту. Дискретные логарифмы.

4 Симметричные алгоритмы.

- ГОСТ 28147-89
- DES
- AES

5 Ассиметричные алгоритмы

- RSA
- ElGamal
- Эллиптические кривые

Сравнение с ассиметричными алгоритмами: вычислительная сложность, длина ключа.

6 Методики подписывания сообщения. MAC. Цифровые подписи.

Хэш-функции. Критерии для криптографически стойких ХФ. Случайные числа. Псевдослучайные числа. Применения ГПСЧ в криптографии. Критерии «случайности» последовательности. История вопроса. Цифровые подписи на основе RSA, ElGamal Дайджесты: MD4, MD5, SHA-1, SHA-256 Время жизни ключей.

7 Методики криптоанализа.

Атака «человек посередине» Атака по боковому каналу (side-channel attack). Социальная инженерия.

8 Блоковые и поточные шифры. Режимы шифрования.

Определения блочных и потоковых шифров, различия между ними. ECB, CBC, CFB, OFB... Вектор инициализации. Различия между режимами: «набивка», трансформация одинаковых блоков, распространение ошибки, возможность распараллеливания.

9 Прочие алгоритмы.

Схемы разделения секретов на базе системы линейных уравнений, интерполяционных многочленов Лагранжа, на основе алгоритма укладки рюкзака. Шифрование и сжатие. Стеганография – не криптография, но прикольно.

10 Криптография в жизни

Политка, государство и защита информации Патенты на алгоритмы. IDEA, Camelia. Реализации алгоримтов: SSL/TLS, SSH, цепочки сертификатов X.509, PGP. Kerberos.

Список литературы

[1] Брюс Шнайер. Прикладная криптография.

[2] Э.М. Габидулин. Лекции по курсу «Защита информации» ФРТК МФТИ.

[3] Дориченко Ященко. 25 этюдов о шифрах.