Алгоритмы и структуры данных

Лекция 13. Алгоритмы шифрования.

(c) Глухих Михаил Игоревич, glukhikh@mail.ru

Алгоритмы шифрования

- По открытости ключа
  - С закрытым ключом
  - С открытым ключом
- По симметричности (ключ шифрации = ключ дешифрации?)
  - Симметричное
  - Асимметричное
- По цели
  - Шифрация
  - Дешифрация
  - Электронная подпись

Шифрование с открытым / закрытым ключом

- Открытый ключ: известен кому угодно, т.е. его не требуется скрывать
  - При этом предполагается, что у получателя сообщения есть ещё закрытый ключ для расшифровки

Шифрование с открытым / закрытым ключом

- Открытый ключ: известен кому угодно, т.е. его не требуется скрывать
  - При этом предполагается, что у получателя сообщения есть ещё закрытый ключ для расшифровки
- Закрытый ключ: известен только двоим участникам передачи (в этом случае возникает отдельный сложный вопрос о передаче закрытого ключа – часто для этого используется алгоритм с открытым ключом)

Шифрование с открытым ключом: принцип

- У получателя есть закрытый ключ (он его придумал или сгенерировал, и никому не показывает)
- Из него он (известным преобразованием) получает открытый ключ и публикует его
  - Преобразование имеет такой характер, что обратное преобразование (открытый ключ → закрытый ключ) намного более трудоёмко
-

Шифрование с открытым ключом: принцип

- У получателя есть закрытый ключ (он его придумал или сгенерировал, и никому не показывает)
- Из него он (известным преобразованием) получает открытый ключ и публикует его
  - Преобразование имеет такой характер, что обратное преобразование (открытый ключ → закрытый ключ) намного более трудоёмко
- Далее, открытый ключ используется для шифрации…
- … а закрытый – для дешифрации

Электронная подпись

- Выполняется в обратном порядке
- Автор документа с помощью закрытого ключа формирует электронную подпись (например, шифруя часть информации в документе)
- Кто угодно другой может проверить его подпись с помощью открытого ключа (расшифровывая и сравнивая с оригиналом)

Шифрование с открытым ключом: RSA

- Алгоритм разработан в 1977 году
  - = Rivest + Shamir + Adleman (три фамилии)
- Базовые функции
  - Открытый → Закрытый ключ: факторизация большого числа
  - Закрытый → Открытый ключ: произведение двух простых чисел
  - Шифрация: возведение в степень по модулю большого числа
  - Дешифрация: вычисление функции Эйлера
    - = количеству натуральных чисел, меньших N и взаимно простых с N

RSA: генерация ключей

- Берём два простых числа (128, 256, 512, 1024, 2048 бит…)
- Считаем их произведение: N = P x Q
- Считаем функцию Эйлера Э(N) = (P-1) x (Q-1)
- Выбираем E, простое или взаимно простое с Э(N) – например, 17, 257, **65537**
- Вычисляем D: (E x D) % Э(N) = 1
  - Обычно для этого используется расширенный алгоритм Евклида
    - E x **D** + Э(N) x **K** = **GCD(E, Э(N))** = 1
- Public key = E, N
- Private key = D

RSA: шифрование

- Сообщение = число в интервале 0…N-1
- Берём исходное сообщение M
- Формируем $C(M) = M^E \% N$

RSA: дешифрование

- Берём принятое C
- Говорим, что $M = U(C) = C^D \% N$

Применение

- Чаще всего с помощью RSA шифруется только ключ для симметричного шифрования
- После чего уже с его помощью передаётся основной текст

Шифрование с закрытым ключом: AES

- AES = Advanced Encryption Standard
- Появление: 2000-2001
- Симметричное шифрование

AES: порядок шифрования

- Выбираем ключ (128, 192 или 256 бит)
- Делим входные данные на блоки по 128 бит (16 байт), каждый из блоков преобразуется в матрицу 4x4 байта
- Выполняется 10, 12 или 14 раундов преобразований матрицы:
  - Перестановка ячеек по фиксированной таблице
  - Сдвиг строк влево
  - Перемножение колонок на фиксированный многочлен
  - XOR для каждой ячейки

AES: порядок дешифрации

- Обратен шифрации

Спасибо за внимание!