# Лабораторная 11

***Хеш-функция*** - математическая или иная функция h=H(M), которая принимает на входе строку символов M(прообраз) переменной длины n и преобразует ее в выходную строку фиксированной длины l (обычно меньшей).

***Хеширование*** - преобразование входного массива данных определенного типа и произвольной длины в выходную битовую строку фиксированной длины.

Преобразования называются хеш-функциями или функциями свертки, а их результаты - хешем, хеш-кодом, хеш-таблицей или дайджестом сообщения.

*Функции хеширования:*

* ***бесконечные хеш-функции***, зависящие только от сообщения
* ***хеш-функции с секретным ключом***, зависящие от сообщения и от секретного ключа

***Криптографическая хеш-функция*** - это специальный класс хеш-функций, который имеет различные свойства, необходимые для решения задач в области криптографии.

*Основные задачи решаемые с помощью хеш-функций:*

* аутентификация(хранение паролей)
* проверка целостности данных
* защита файлов
* обнаружение зловредного ПО
* криптовалютные технологии

*Свойства хеш-функция:*

1. ***Детерминированность***: независимо сколько раз вычисляется H(M), M - const, при использовании одинакового алгоритма код хеш-преобразования h всегда должен быть одинаковым.
2. ***Скорость вычисления хеша h***: процесс вычисления h медленный, система - неэффективная
3. ***Сложность обратного вычисления***: для известного H(M) невозможно определить M (свойство односторонности преобразования)
4. Минимальные изменения в хешируемых данных(M!=M) должны изменять хеш: H(M)!=H(M`)

***Коллизия хеш-функции Н*** - ситуация при которой различным входам( в общем случае x и y или M!=M`) соответствует одинаковый хеш-код: H(x) = H(y) или H(M) = H(M`)

1. ***Коллизионная устойчивость***. Зная M, трудно найти такое M` (M!=M`), для которого H(M)=H(M`). Если равенство выполняется, то - *коллизия 1-го рода*. Если случайным образом выбраны два сообщения (M и M`), для которых H(M)=H(M`), говорят о *коллизии 2-го рода*. Поиск коллизий основан на задаче - “Парадоксе дня рождения”

Парадокс гласит:

Если в группе есть 23 человека то с вероятностью в 50% двое из них родились в один день. Парадоксом является высокая вероятность наступления указанного события. При этом:

* в группе нет близнецов
* люди рождаются равномерно и случайно. Это значит люди с равной вероятностью могут рождаться в любой день года. 1/365
* рождаются независимо друг от друга, дата рождения одного не влияет на дату рождения другого

Существует m возможных дней рождения, а группа состоит из n человек. Тогда :

**P(An) = P(An-1) \* ((m-(n-1))/m**

Хеш-функция - это функция, выполняющая отображение из множества М в число, находящееся в интервале [0, m-1]: h:M -> [0, m-1]

Стойкость к коллизии означает, что трудно найти такие Mi и Mj (Mi, Mj принадлежит M), при которых h(Mi)=h(Mj), i!=j, 1<=i, j<=n

В атаке m - количество календарных дней в году, М - множество людей, составляющих группу.

Люди хешируются в их дни рождения, которые могут быть одним из значений m.

Задача состоит в том чтобы определить наименьшее n при котором хеш двух значений m будет “одним днем рождения” n = (2m ln100)^½

## Хеш-функции:

* MD2/4/5/6
* SHA-1, SHA-2(собирательное - SHA-224, SHA-256, SHA-384, SHA-512), SHA-3 - использует конструкцию “криптографическая губка” - итеративный подход для создания функции с произвольной длиной на входе и произвольной длиной на выходе
* ГОСТ 34.11-94

### MD

Входное сообщение максимальной длины 2^64-1 битов преобразуют в хеш длиной l=128 битов. Исключение 6-я версия длины хеша от 1 до 512 бит

### SHA

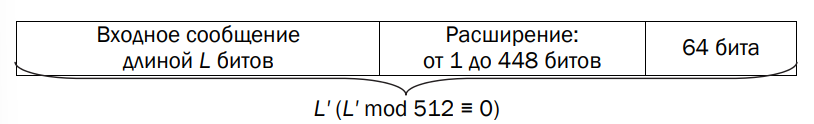
Максимальный объем хешируемых сообщений такой же что и для MD.

Длина хешей: SHA-1 - 160 битов, SHA-2 - соответствует числу дополняющему через дефис название алгоритма. Максимальная длина SHA-512, 384, 512/256, 512/224 - соответствует 2^128-1 битов

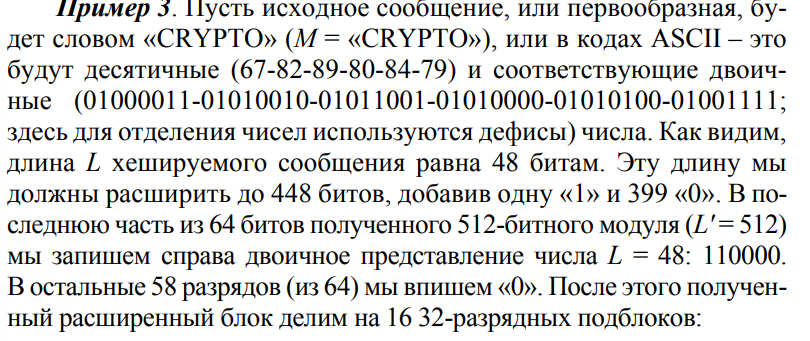
Оба алгоритма разделяются на 5 стадий:

* расширение входного сообщения
* разбивка расширенного сообщения на блоки
* инициализация начальных констант
* обработка сообщения поблочно
* вывод результата

Сообщение расширяется так чтобы итоговая длина была кратна 512



Основа алгоритмов - модуль, состоящий из циклических преобразований каждого 512-битного блока, который делится на подблоки длиной 32 либо 64 бита



#### *MD4*

Весь алгоритм состоит из 3-х раундов.

В каждом из раундов выполняется 16 шагов(по числу подблоков).

Каждый шаг вычисляется нелинейную функцию над 3-мя переменными из {a, b, c, d}.

В каждом раунде своя нелинейная функция

При создании хеш-функции используются:

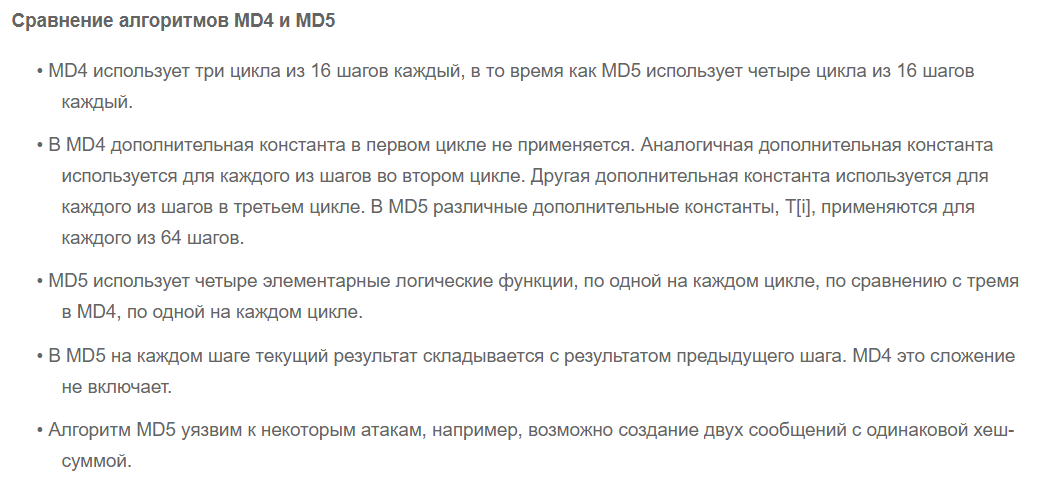
* операция логического суммирования OR - дизъюнкция +
* операция логического умножения AND - конъюнкция .
* операция отрицания NOT
* операция логического сдвига на s разрядов
* операция суммирования по модулю 2

#### MD5

добавлен 4-ый раунд, на каждом раунде и шаге используется уникальная константа t

результат каждого раунда добавляется к предыдущему

порядок следования подблоков изменяется в 2 и 3 раундах



#### SHA1

Длина сообщения максимум 2^64-1

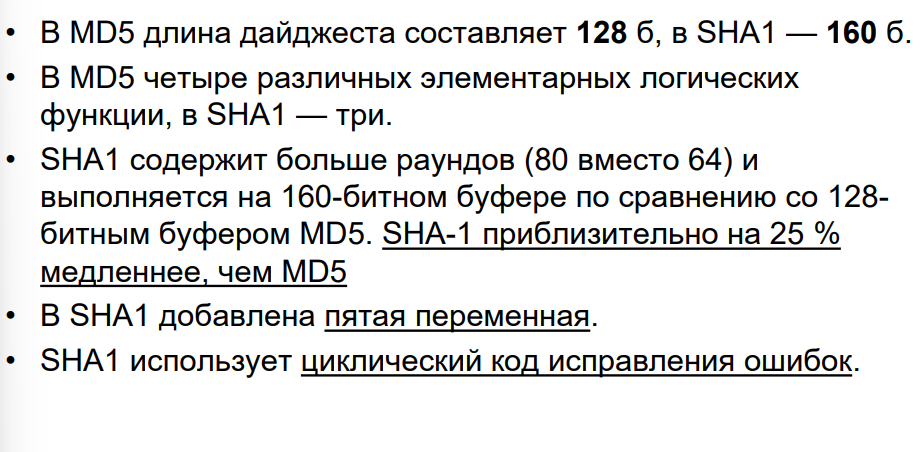
Генерирует 160-битное хеш-значение

Четыре этапа

Каждое действие прибавляется к ранее полученному результату

Размер блока обработки равен 512 бит

Сложение по модулю 2^32



# Лабораторная 12

***ЭЦП*** - контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства

ЭЦП выполняет те же функции что и обычная подпись:

**ЭЦП - бинарная последовательность, зависит от содержания подписываемого сообщения**

ЭЦП может быть реализована на основе:

* **симметричных систем**( с тайным ключом) - не отличается от DES
* **симметричных систем и посредника** - создаются две симметричные системы: между отправителем и посредником, посредником и получателем. Посредник выдает двум сторонам совершенно разные тайные ключи
* **асимметричных систем**(с открытым ключом) - сообщение шифруется тайным ключом отправителя, отправитель верифицирует подпись(устанавливает авторство - для расшифрования публичный ключ отправителя, гарантия надежности если после расшифрования формат и содержимое документа имеют логическую стойкость) с помощью своего открытого ключа.

***ЭЦП*** - бинарная последовательность символов, являющаяся реквизитом электронного документа, зависящая от содержания этого документа и предназначенная для подтверждения целостности и подлинности электронного документа

## ЭЦП на основе хешей подписываемых сообщений

Предусматривает подписание не сообщения а его хеша.

Это сокращает время генерации/верификации подписи и снижает вероятность появления случайных ошибок в итоговом документе

Важное свойство эцп - возможность ее проверить есть у каждого кто имеет доступ к открытому ключу автора.

Если H(Mп) = H(Mo) - то подпись подлинная и документ целостный

* при генерации ЭЦП отправитель последовательно выполняет действия:
  + вычисление хеша сообщения
  + вычисление содержимого ЭЦП(S) по хешу с использованием закрытого ключа d: S=Cd(H(M))
  + присоединение ЭЦП к сообщению M - получая сообщение M’
  + отправление сообщение M’ получателю
* получатель
  + отделяет цифровую подпись S от сообщения M
  + применяет к сообщению M функцию хеширования - получает образ полученного сообщения
  + использует открытый ключ отправителя расшифровывает ЭЦП S извлекает из нее хеш-образ отправленного сообщения
  + проверяет соответствие обоих хеш-образов

## ЭЦП на основе RSA

две ситуации

* сообщение подписывается и передается в открытом виде
* сообщение подписывается и передается в зашифрованном виде

Отправитель шифрует документ своим закрытым ключом C = F(M; da; na)

Получатель расшифровывает открытым ключом отправителя M = F(C; ea, na)

***Вычисление подписи***

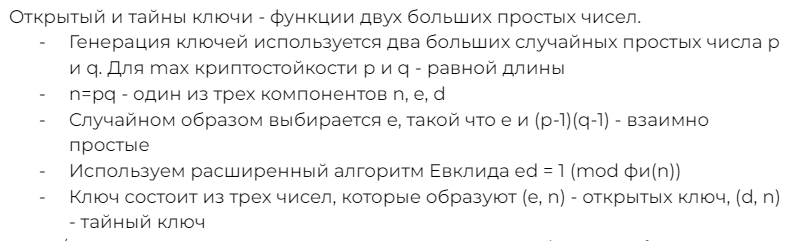


d0, n0 - элементы тайного ключа отправителя

Расшифрование получатель



Вычисляется H(Mп). Если H(M0) = H(Mп) - подпись верифицирована



Если сообщение в зашифрованном виде - то отправитель шифрует открытым ключом получателя, который перед процессом верификации подписи расшифровывает послание своим тайным ключом

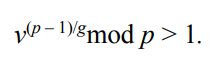
## 

## ЭЦП на основе DSA

p - простое число длиной от 64 до 1024 битов(кратно 64)

q - 160-битный простой множитель (р-1)

Вычисляется g: 

v - любое число, меньше (p-1) для которого выполняется условие - 

Еще один элемент ключа **y** вычисляется  открытый ключ, где x < q; x - закрытый ключ

### Генерация ЭЦП сообщения

H(m) – хеш подписываемого сообщения

ЭЦП - из двух чисел: r и s

Число k - как в шифре Эль-Гамаля

Отправитель:

* Генерация ключей: выбираем x(закрытый) вычисляем y(открытый)
* Вычисляем хеш сообщения h=H(m)
* Формируем ЭЦП - выбираем случайное k<q: r=(g^k mod p) mod q; s = ((h-xr)/k) mod q

Получатель:

* Получает письмо с ЭЦП (m, r, s)
* Считаем:
  + w = s^-1 mod q
  + u1 = (H(m)\*w) mod q
  + u2 = (rw) mod q
  + a = ((g^u1 \* g^u2) mod p) mod q
* Если a = r - эцп верна

## ЭЦП Эль-Гамаля

Отличие от DSA - результат зашифрования одна пара чисел, а не пара для каждого блока исходного сообщения

### Генерация ключа

Открытый ключ - y g p

Тайный ключ - x

Выбираем k взаимно простое с p-1

Вычисляем числа a, b - являющиеся ЭЦП S = {a, b}

a = g^k mod p

Для вычисления b - при помощи расширенного алгоритма Евклида решается уравнение H(M0) = (xa + kb) mod (p-1)

Получателю отправляем M’=Mo||S

### Верификация подписи

Вычисляется хеш полученного сообщения H(Mп) = h

И проверить выполняется ли равенство : y^a a^b = g^h mod p

## ЭЦП Шнорра

Особенность Э-Г число p - должно быть большим

Шнор предложи:

p - простое число в диапазоне от 512 до 1024 битов

q - 160-битное простое число делителитель (p-1)

g - любое число g(g!=1) такое что 

Открытый ключ - p, g, q

Выбирается число x<q(тайный ключ) и вычисляется последний элемент открытого ключа 

Длина секретного ключа 160 битов

Для подписи сообщения Мо выбирается случайное число k (1<k<q) и вычисляется а:



Вычисляется хеш от конкатенации сообщения Мо и числа а(создается хеш-образ подписываемого сообщения спереди присоединенного к числу а) Далее вычисляет значение b: 

Получателю отправляется сообщение M’=Мо||S

Получатель проверяет подпись 

Затем проверяет выполняется ли равенство: h=H(Mп||Х) - подпись достоверна если равенство выполняется