Лекция 5. HASH-функция SHA-1

Определение HASH-функции

HASH-функция (хеширование) — преобразование по детерминированному алгоритму входного массива данных произвольной длины в выходную битовую строку фиксированной длины.

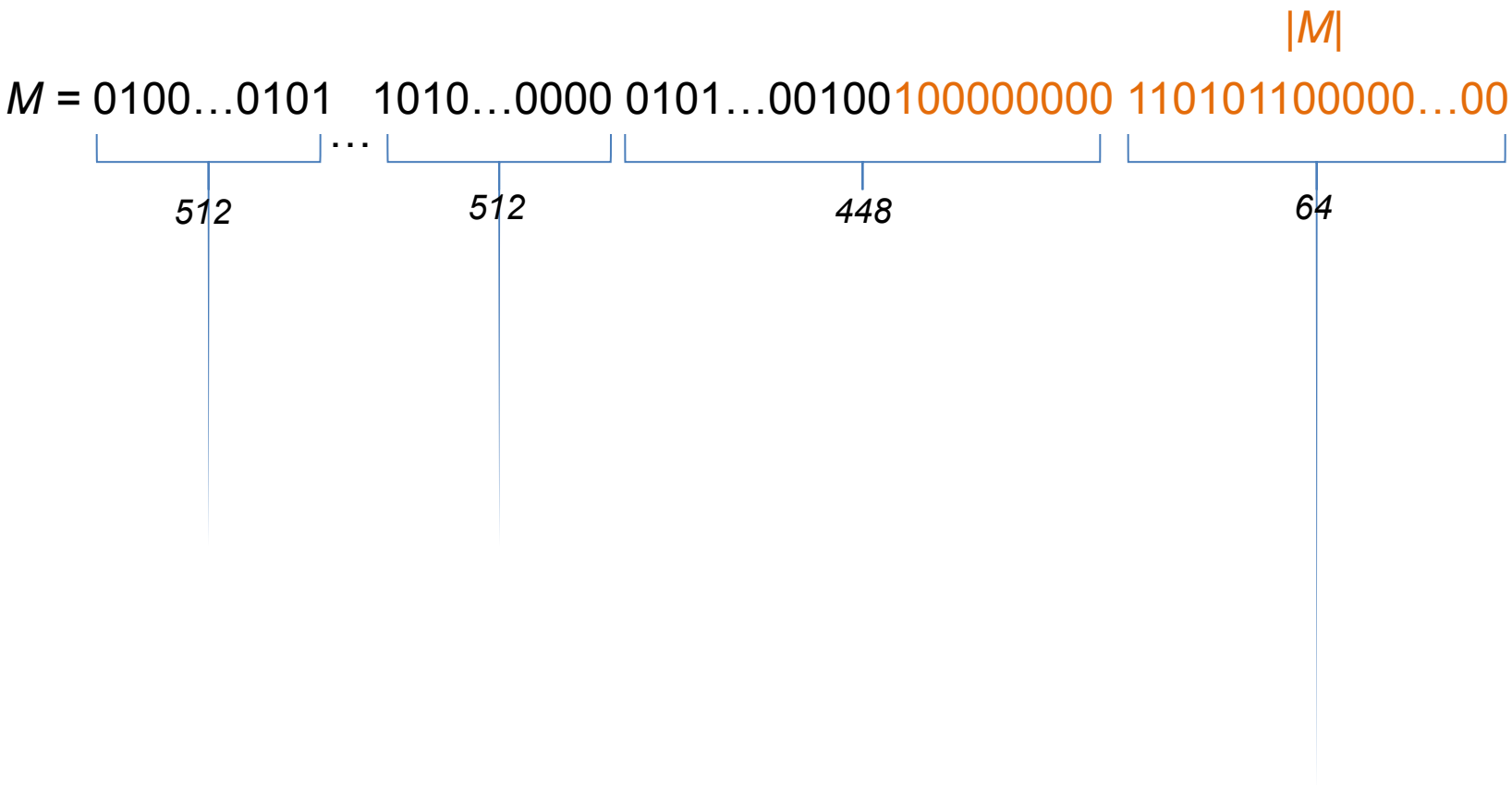
Свойства HASH-функций:

1. **Необратимость - найти обратной значение вычислительно-сложно ($f(x)=y$ – вычислить легко, но $f^{-1}(y)=x$ вычислить сложно).**
2. **Стойкость к колизиям I и II группы.**
3. **Быстрая вычисляемость.**
4. **Лавинный эффект.**

HASH-функция SHA-1.

- ✔ 160-битный алгоритм хэширования;
- ✔ Опубликован в 1995 году;
- ✔ Рекомендован в качестве основного для государственных учреждений в США;
- ✔Раундовый, 80 раундов;
- ✔Блоковый, блок – 512 бит.

Дополнение сообщения до длины, кратной 512 битам



Инициализация переменных

Определяются 10 буферных переменных:

A = a = 0x67452301
B = b = 0xEFCDAB89
C = c = 0x98BADCFE
D = d = 0x10325476
E = e = 0xC3D2E1F0

Определяются четыре нелинейные операции и четыре константы:

$F_t(m,l,k) = (m \wedge l) \vee (\neg m \wedge k)$	K_t = 0x5A827999	0≤t≤19
$F_t(m,l,k) = m \oplus l \oplus k$	K_t = 0x6ED9EBA1	20≤t≤39
$F_t(m,l,k) = (m \wedge l) \vee (m \wedge k) \vee (l \wedge k)$	K_t = 0x8F1BBCDC	40≤t≤59
$F_t(m,l,k) = m \oplus l \oplus k$	K_t = 0xCA62C1D6	60≤t≤79

Задача. Переведите в шестнадцатеричную систему вектор

1011 1110 1101 1010 0010 0000 0001 0100 = 0x… ?

Задача. Переведите в шестнадцатеричную систему вектор

1011 1110 1101 1010 0010 0000 0001 0100 = 0xbeda2014

Главный цикл обработки 512-битового блока

Блок сообщения преобразуется из 16 32-битовых слов M_i в 80 32-битовых слов W_i по следующему правилу:

$$W_t = M_t \quad \text{при } 0 \le t \le 15$$
$$W_t = (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_{t-16}) << 1 \quad \text{при } 16 \le t \le 79$$

далее:

для t **от** 0 **до** 79
temp = (a<<5) + F_t(b,c,d) + e + $W_t + K_t$
e = d
d = c
c = b<<30
b = a
a = temp

A=A+a D=D+d
B=B+b E=E+e
C=C+c

Главный цикл. Графическая схема.

для t **от** 0 **до** 79

temp = (a<<5) + F_t(b,c,d) + e + $W_t + K_t$

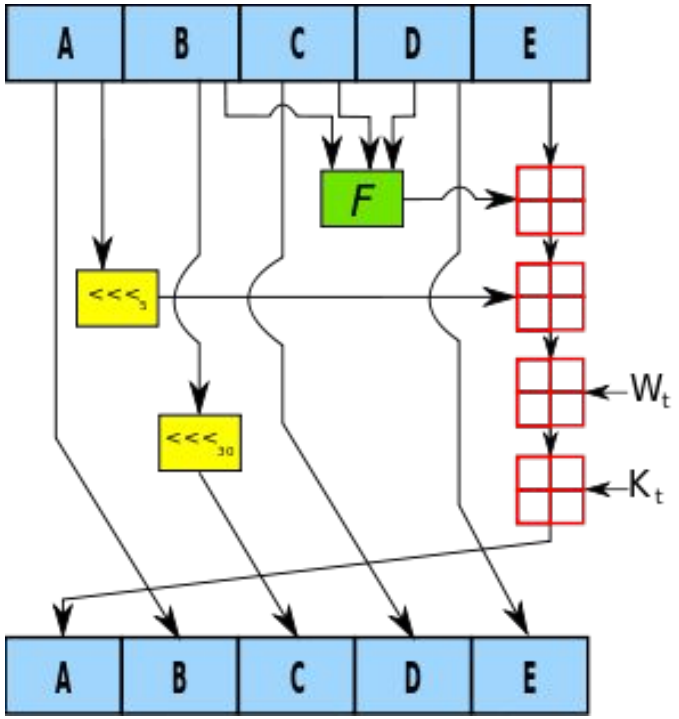
e = d

d = c

c = b<<30

b = a

a = temp



Пример

SHA-1("В чащах юга жил бы цитрус? Да, но фальшивый экземпляр!") =
9e32295f 8225803b b6d5fdfc c0674616 a4413c1b

SHA-1("") =
da39a3ee 5e6b4b0d 3255bfef 95601890 afd80709

Использование

- ✔SHA-1 используется в следующих приложениях:
- ✔S/MIME — дайджесты сообщений.
- ✔SSL — дайджесты сообщений.
- ✔IPSec — для алгоритма проверки целостности в соединении «точка-точка».
- ✔SSH — для проверки целостности переданных данных.
- ✔PGP — для создания электронной цифровой подписи.
- ✔Git — для идентификации каждого объекта по SHA-1-хешу от хранимой в объекте информации.
- ✔Mercurial — для идентификации ревизий
- ✔BitTorrent — для проверки целостности загружаемых данных.