



数据结构与算法 (Python) –05+/MD5

刘云淮 Yunhuai.liu@pku.edu.cn

<http://www.yunhuai.net/DSA2025/CoursePage/DSA2025.html>

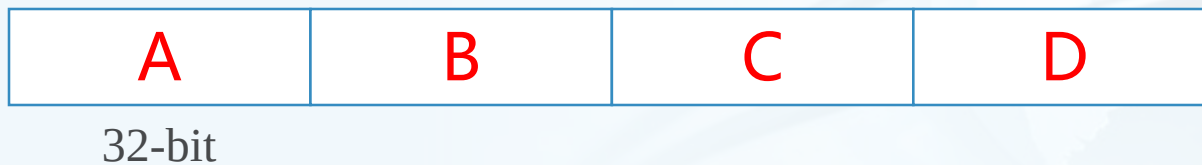
北京大学计算机学院

MD5 描述和准备阶段

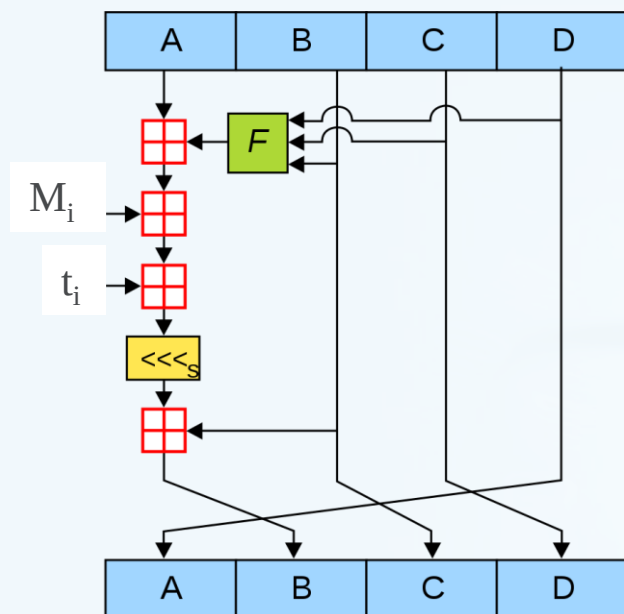
- 工作于上512位块的消息
- 产生的128位列码
- 填充(Padding)
 - 信息被填充为 512 位数据块的精确倍数
 - 信息中添加 1
 - 剩余部分（少于 64 位）根据需要填充 0
 - 最后 64 位用于表示信息长度
- 区块细分
 - 细分为若干 512 位数据块

基本思想

- 从恒定的 128 位状态开始
- 分为四个 32 位字，分别表示为 A、B、C 和 D
- 每个 512 位数据块将被划分为 16 个 32 位数据块
- 每个 32 位块将用来修改 128 位状态 16 次
- 每 16 次操作称为一轮
- 4 轮，操作略有不同



每个轮此的主要操作（16个操作一个轮次）



Block 1

Block 2

Block 3

Block 4

⋮

Block 16

初始的ABCD字符串

A = 0x01234567

B = 0x89abcdef

C = 0xfedcba98

D = 0x76543210

非线性生成函数 (Nonlinear Generating Functions)

$$F(B, C, D) = (B \wedge C) \vee (\neg B \wedge D)$$

$$G(B, C, D) = (B \wedge D) \vee (C \wedge \neg D)$$

$$H(B, C, D) = B \oplus C \oplus D$$

$$I(B, C, D) = C \oplus (B \vee \neg D)$$

$\text{FF}(a, b, c, d, M_j, s, t_i)$ denotes $a = b + ((a + F(b, c, d) + M_j + t_i) \lll s)$

$\text{GG}(a, b, c, d, M_j, s, t_i)$ denotes $a = b + ((a + G(b, c, d) + M_j + t_i) \lll s)$

$\text{HH}(a, b, c, d, M_j, s, t_i)$ denotes $a = b + ((a + H(b, c, d) + M_j + t_i) \lll s)$

$\text{II}(a, b, c, d, M_j, s, t_i)$ denotes $a = b + ((a + I(b, c, d) + M_j + t_i) \lll s)$

一些重要的常量

$\text{FF}(a,b,c,d,M_j,s,t_i)$ denotes $a = b + ((a + F(b,c,d) + M_j + t_i) \lll s)$

$\text{GG}(a,b,c,d,M_j,s,t_i)$ denotes $a = b + ((a + G(b,c,d) + M_j + t_i) \lll s)$

$\text{HH}(a,b,c,d,M_j,s,t_i)$ denotes $a = b + ((a + H(b,c,d) + M_j + t_i) \lll s)$

$\text{II}(a,b,c,d,M_j,s,t_i)$ denotes $a = b + ((a + I(b,c,d) + M_j + t_i) \lll s)$

M_j 是信息块的第 j 个子块。

对于第 i 步

$t_i = 232 * \text{abs}(\sin(i))$ 其中 i 以弧度为单位。

s 是要移位的位数：

Round 1: [7, 12, 17, 22]

Round 2: [5, 9, 14, 20]

Round 3: [4, 11, 16, 23]

Round 4: [6, 10, 15, 21]

Round 1

```
FF (a, b, c, d, M0, 7, 0xd76aa478)
FF (d, a, b, c, M1, 12, 0xe8c7b756)
FF (c, d, a, b, M2, 17, 0x242070db)
FF (b, c, d, a, M3, 22, 0xc1bdceee)
FF (a, b, c, d, M4, 7, 0xf57c0faf)
FF (d, a, b, c, M5, 12, 0x4787c62a)
FF (c, d, a, b, M6, 17, 0xa8304613)
FF (b, c, d, a, M7, 22, 0xfd469501)
FF (a, b, c, d, M8, 7, 0x698098d8)
FF (d, a, b, c, M9, 12, 0x8b44f7af)
FF (c, d, a, b, M10, 17, 0xffff5bb1)
FF (b, c, d, a, M11, 22, 0x895cd7be)
FF (a, b, c, d, M12, 7, 0x6b901122)
FF (d, a, b, c, M13, 12, 0xfd987193)
FF (c, d, a, b, M14, 17, 0xa679438e)
FF (b, c, d, a, M15, 22, 0x49b40821)
```


Round 2

```
GG (a, b, c, d, M1, 5, 0xf61e2562)
GG (d, a, b, c, M6, 9, 0xc040b340)
GG (c, d, a, b, M11, 14, 0x265e5a51)
GG (b, c, d, a, M0, 20, 0xe9b6c7aa)
GG (a, b, c, d, M5, 5, 0xd62f105d)
GG (d, a, b, c, M10, 9, 0x02441453)
GG (c, d, a, b, M15, 14, 0xd8a1e681)
GG (b, c, d, a, M4, 20, 0xe7d3fbc8)
GG (a, b, c, d, M9, 5, 0x21e1cde6)
GG (d, a, b, c, M14, 9, 0xc33707d6)
GG (c, d, a, b, M3, 14, 0xf4d50d87)
GG (b, c, d, a, M8, 20, 0x455a14ed)
GG (a, b, c, d, M13, 5, 0xa9e3e905)
GG (d, a, b, c, M2, 9, 0xfcefa3f8)
GG (c, d, a, b, M7, 14, 0x676f02d9)
GG (b, c, d, a, M12, 20, 0x8d2a4c8a)
```

Round 3

```
HH (a, b, c, d, M5, 4, 0xffffa3942)
HH (d, a, b, c, M8, 11, 0x8771f681)
HH (c, d, a, b, M11, 16, 0x6d9d6122)
HH (b, c, d, a, M14, 23, 0xfde5380c)
HH (a, b, c, d, M1, 4, 0xa4beea44)
HH (d, a, b, c, M4, 11, 0x4bdecfa9)
HH (c, d, a, b, M7, 16, 0xf6bb4b60)
HH (b, c, d, a, M10, 23, 0xbebfbcb70)
HH (a, b, c, d, M13, 4, 0x289b7ec6)
HH (d, a, b, c, M0, 11, 0xea127fa)
HH (c, d, a, b, M3, 16, 0xd4ef3085)
HH (b, c, d, a, M6, 23, 0x04881d05)
HH (a, b, c, d, M9, 4, 0xd9d4d039)
HH (d, a, b, c, M12, 11, 0xe6db99e5)
HH (c, d, a, b, M15, 16, 0x1fa27cf8)
HH (b, c, d, a, M2, 23, 0xc4ac5665)
```

Round 4

$\Pi(a, b, c, d, M_0, 6, 0xf4292244)$
 $\Pi(d, a, b, c, M_7, 10, 0x432aff97)$
 $\Pi(c, d, a, b, M_{14}, 15, 0xab9423a7)$
 $\Pi(b, c, d, a, M_5, 21, 0xfc93a039)$
 $\Pi(a, b, c, d, M_{12}, 6, 0x655b59c3)$
 $\Pi(d, a, b, c, M_3, 10, 0x8f0ccc92)$
 $\Pi(c, d, a, b, M_{10}, 15, 0xffeff47d)$
 $\Pi(b, c, d, a, M_1, 21, 0x85845dd1)$
 $\Pi(a, b, c, d, M_8, 6, 0x6fa87e4f)$
 $\Pi(d, a, b, c, M_{15}, 10, 0xfe2ce6e0)$
 $\Pi(c, d, a, b, M_6, 15, 0xa3014314)$
 $\Pi(b, c, d, a, M_{13}, 21, 0x4e0811a1)$
 $\Pi(a, b, c, d, M_4, 6, 0xf7537e82)$
 $\Pi(d, a, b, c, M_{11}, 10, 0xbd3af235)$
 $\Pi(c, d, a, b, M_2, 15, 0x2ad7d2bb)$
 $\Pi(b, c, d, a, M_9, 21, 0xeb86d391)$

如果你觉得你也能破解，你可以试试！