代码思路:

根据百度百科的查找之后了解到 SHA-256 算法输入报文的最大长度不超过 2^64 bit,输入按 512-bit 分组进行处理,产生的输出是一个 256-bit 的报文。该算法处理包括以下几步:

1: 附加填充比特。对报文进行填充使报文长度与 448 模 512 同余(长度=448 mod 512),填充的比特数范围是 1 到 512,填充比特串的最高位为 1,其余位为 0。

就是先在报文后面加一个 1, 再加很多个 0, 直到长度 满足 mod 512=448.

为什么是 448, 因为 448+64=512. 第二步会加上一个 64bit 的 原始报文的 长度信息。

- 2: 附加长度值。将用 64-bit 表示的初始报文(填充前)的位长度附加在步骤 1 的结果后(低位字节优先)。
- 3: 初始化缓存。使用一个 256-bit 的缓存来存放该散列函数的中间及最终结果。 该缓存表示为 A=0x6A09E667, B=0xBB67AE85, C=0x3C6EF372, D=0xA54FF53A, E=0x510E527F, F=0x9B05688C, G=0x1F83D9AB, H=0x5BE0CD19。
- 4: 处理 512-bit(16 个字)报文分组序列。该算法使用了六种基本逻辑函数,由 64 步迭代运算组成。每步都以 256-bit 缓存值 ABCDEFGH 为输入,然后更新缓存内容。每步使用一个 32-bit 常数值 Kt 和一个 32-bit Wt。

输出结果:

Microsoft Visual Studio 调试控制台

Sha256: h0 h1 h2 h3 h4 h5 h6 h7 D: \山东大学\专业课\创新创业实践\Project1\x64\Debug\Project1.exe(进程 5496)已退出,代码为 0。 要在调试停止时自动关闭控制台,请启用"工具"->"选项"->"调试"->"调试停止时自动关闭控制台" 按任意键关闭此窗口.....