我们将在表 13-8 中更详细地讨论摘要认证中那些特殊的首部。

13.1.2 单向摘要

摘要是“对信息主体的浓缩”。[6] 摘要是一种单向函数，主要用于将无限的输入值转换为有限的浓缩输出值。[7] 常见的摘要函数 MD5，[8] 会将任意长度的字节序列转换为一个 128 位的摘要。

128 位 = 2^{128}，或者大约

288 1 000 000 000 000 000 000 000 000 000 000 000 000 种不同的输出值。

对这些摘要来说，最重要的是如果不知道密码的话，要想正确地猜出发送给服务器的摘要将是非常困难的。同样，如果有摘要，想要判断出它是由无数输入值中的哪一个产生的，也是非常困难的。

MD5 输出的 128 位的摘要通常会被写成 32 个十六进制的字符，每个字符表示 4 位。表 13-1 给出了几个示例输入的 MD5 摘要。注意 MD5 是怎样根据任意的输入产生定长的摘要输出的。

表13-1 MD5摘要实例

输　入	MD5摘要
"Hi"	C1A5298F939E87E8F962A5EDFC206918
"bri:Ow!"	BEAAA0E34EBDB072F8627C038AB211F8
"3.1415926535897"	475B977E19ECEE70835BC6DF46F4F6DE
"http://www.http-guide.com/index.htm"	C617C0C7D1D05F66F595E22A4B0EAAA5
"WE hold these Truths to be self-evident, that all Men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the Pursuit of Happiness—That to secure these Rights, Governments are instituted among Men, deriving their just Powers from the Consent of the Governed, that whenever any Form of Government becomes destructive of these Ends, it is the Right of the People to alter or to abolish it, and to institute new Government, laying its Foundation on such Principles, and organizing its Powers in such Form, as to them shall seem most likely to effect their Safety and Happiness."	66C4EF58DA7CB956BD04233FBB64E0A4

注 6：韦氏词典，1998 年。

注 7：理论上来讲，我们将数量无限的输入值转换成了数量有限的输出值，所以两个不同的输入值就可能映射为同一个摘要。这种情况被称为*冲突*（collision）。实际上，由于可用输出值的数量足够大，所以在现实生活中，出现冲突的可能是微乎其微的，对我们要实现的密码匹配来说并不重要。

注 8：MD5 表示“报文摘要的第五版”，是摘要算法系列中的一种。*安全散列算法*（Secure Hash Algorithm，SHA）是另一种常见的摘要函数。