我们来证实一个简单的检验和（如因特网检验和）只能算作劣质的密码散列函数。不像在因特网检验和中执行反码运算那样，我们把每个字符看作一个字节，并把这些字节加到一起，一次用4字节的块来进行计算。假定Bob欠Alice 100.99美元并且向Alice发送一张借据，这个借据包含以下文本字符串“IOU100.99BOB”。这些字符的ASCII表示（以十六进制形式表示）为49，4F，55，31，30，30，2E，39，39，42，4F，42。

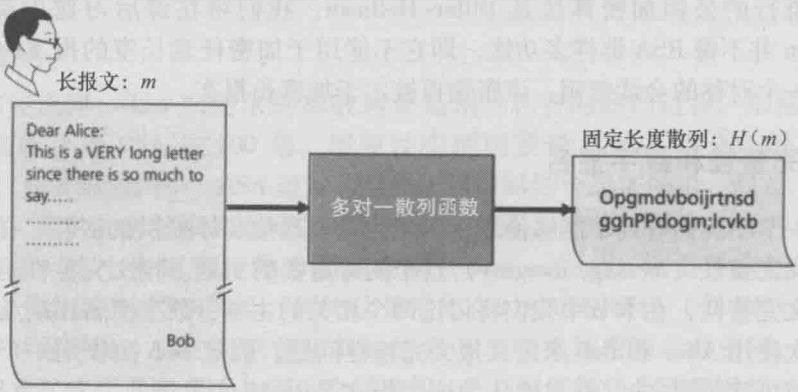

图8-7 散列函数

图8-8上半部分显示了这个报文的4字节检验和是B2 C1 D2 AC。图8-8下半部分显示了一条稍微不同的报文（但是Bob要付的钱却多了许多）。报文“IOU100.99BOB”和“IOU900.19BOB”有相同的检验和。因此，这种简单的检验和算法违反了上述的要求。给定初始数据，很容易找到有相同检验和的另一组数据。很明显，为了安全起见，我们需要比检验和更为强有力的散列函数。

Ron Rivest［RFC 1321］的MD5散列算法如今正在广泛使用。这个算法通过4步过程计算得到128比特的散列。这4步过程由下列步骤组成：①填充——先填1，然后填足够多的0，直到报文长度满足一定的条件；②添加——在填充前添加一个用64比特表示的报文长度；③初始化累加器；④循环——在最后的循环步骤中，对报文的16字块进行4轮处理。MD5的描述（包括一个C源代码实现）可参见［RFC 1321］。

报文	ASCII表示				
I O U 1	49	4F	55	31	
0 0 . 9	30	30	2E	39	
9 B O B	39	42	4F	42	
	B2	C1	D2	AC	检验和

报文	ASCII表示				
I O U 9	49	4F	55	39	
0 0 . 1	30	30	2E	31	
9 B O B	39	42	4F	42	
	B2	C1	D2	AC	检验和

图8-8 初始报文和欺诈报文具有相同的检验和

目前正使用的第二个主要报文摘要算法是安全散列算法SHA-1（Security Hash Algorithm）［FIPS 1995］。这个算法的原理类似于MD4［RFC 1320］设计中所使用的原理，而MD4是MD5的前身。SHA-1是美国联邦政府的标准，任何联邦政府的应用程序如果需要使用密码散列算法的话，都要求使用SHA-1。SHA-1生成一个160比特的报文摘要。较长的输出长度可使SHA-1更安全。

8.3.2 报文鉴别码

我们现在再回到报文完整性的问题。既然我们理解了散列函数，就先来看一下将如何