实验二　Crypto_Hash 实验

一、实验背景

密码散列函数（英语：Cryptographic hash function），又译为加密散列函数、密码散列函数、加密散列函数，是散列函数的一种。它被认为是一种单向函数，也就是说极其难以由散列函数输出的结果，回推输入的数据是什么。这样的单向函数被称为“现代密码学的驮马”。[1]这种散列函数的输入数据，通常被称为消息（message），而它的输出结果，经常被称为消息摘要（message digest）或摘要（digest）。

一个理想的密码散列函数应该有四个主要的特性：

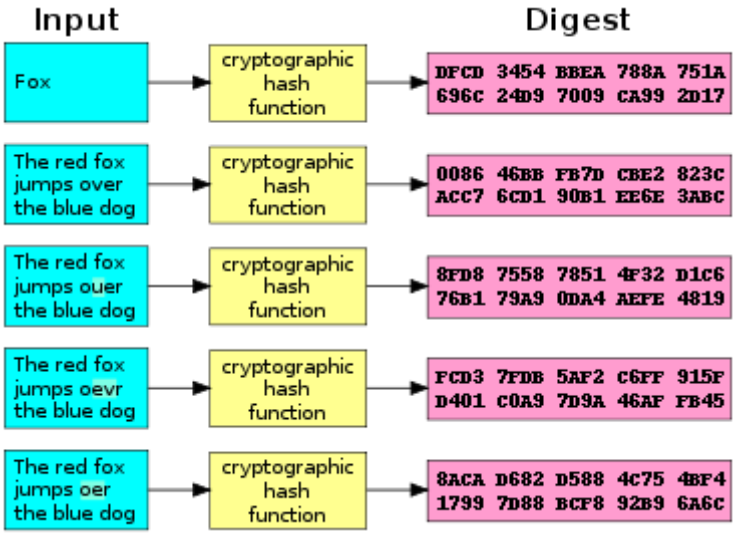
对于任何一个给定的消息，它都很容易就能运算出散列数值

难以由一个已知的散列数值，去推算出原始的消息

在不更动散列数值的前提下，修改消息内容是不可行的

对于两个不同的消息，它不能给与相同的散列数值

在信息安全中，有许多重要的应用，都使用了密码散列函数来实现，例如数字签名，消息认证码。



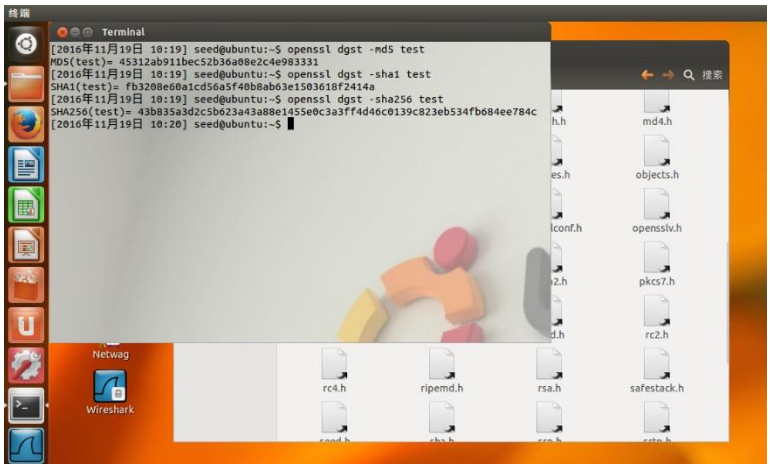
二、实验环境及过程

实验环境为在 VM 虚拟机中运行的 SEEDUbuntu12.04 系统（系统已经由实验室配置好环境）。

实验过程参考该实验下提供的 PDF 的实验指导书完成。

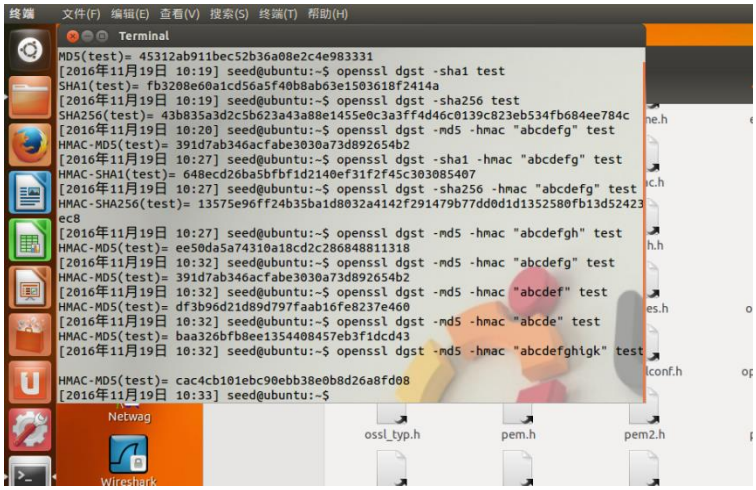
三、实验过程

对指定的文件进行加密，获取信息摘要和认证码。至少使用三种不同的加密算法（如-md5, -sha1, -sha256 等）



加密同一文件得到不同 MAC

对同一文件利用同一种算法进行关键字长度不同的 HMAC 散列函数进行加密，获取信息摘要和认证码



不同长度的加密得到不同 MAC

四、实验总结

通过此次实验，了解 Crypto_Hash 哈希加密的方法，使自己对哈希函数散列值和消息认证码有一定的认识和了解，同时学会使用 SEEDLABS 网站进行网络安全的网上学习，提高自主学习的能力。

实验心得

通过此次实验，我对 Heartbleed 漏洞有了一定的认识，了解了利用该漏洞的攻击手段及修复方式，进行了简单的 Heartbleed 漏洞攻击，成功的获得了预期的数据，并在指导书的帮助下完成了漏洞的修复；

对 Crypto_Hash 哈希加密算法有了一定的认识，熟悉了单向散列函数和消息认证码，对 Crypto_Hash 有了更深层次的了解。同时，我也学会了如何在网上进行自主学习，对我的自主学习能力有了一定的提升。当然，此次实验也暴露了一些问题。一是实验指导书为纯英文，我做起实验来十分费劲，很多地方需要通过猜测进行实验，导致我对实验的理解没有上升到应有的高度。

感谢 Seedlab,这是一个很好的实验平台。将会继续完成。