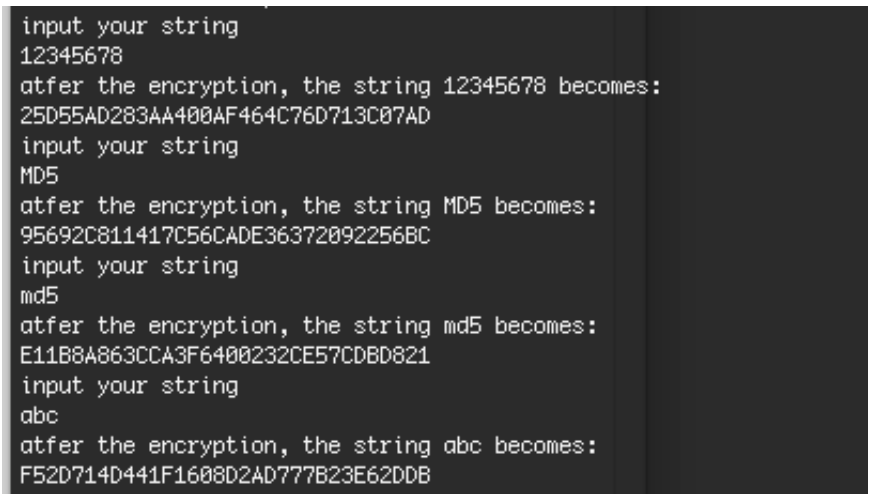
MD5实验报告

实验结果



How MD5 works for password protection

1. 任意长度数据的MD5值长度都是固定长度的。
2. 数据任意的改动，只要修改一个字节，MD5值都会有很大的区别。
3. 要获得两个MD5值一样的数据，是十分困难的。

综上，MD5保护密码的方法可以使这样的：

例如在提交密码与服务器端进行验证的时候，客户端输入密码的时候，向服务端提交的是密码的MD5值，而不是密码明文。在服务端进行验证的时候，服务端随机生成一个salt值，然后再通过MD5验证salt+MD5(password)的值，然后得到的值域数据库密码进行对比。从而避免了密码的明文传输，保证了密码的安全。