

# MD5实验报告

## 实验结果

```
input your string
12345678
after the encryption, the string 12345678 becomes:
25D55AD283AA400AF464C76D713C07AD
input your string
MD5
after the encryption, the string MD5 becomes:
95692C811417C56CADE36372092256BC
input your string
md5
after the encryption, the string md5 becomes:
E11B8A863CCA3F6400232CE57CDBD821
input your string
abc
after the encryption, the string abc becomes:
F52D714D441F1608D2AD777B23E62DDB
```

## 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。