## hex和base32和base64的区别与联系

hex也称为base16，意思是使用16个可见字符来表示一个二进制数组，编码后数据大小将翻倍,因为1个字符需要用2个可见字符来表示。

base32，意思是使用32个可见字符来表示一个二进制数组，编码后数据大小变成原来的8/5,也即5个字符用8个可见字符表示，但是最后如果不足8个字符，将用=来补充。

base64，意思是使用64个可见字符来表示一个二进制数组，编码后数据大小变成原来的4/3,也即3个字符用4个可见字符来表示。

## 关于加密算法的一些分类

1:消息摘要：（数字指纹）：既对一个任意长度的一个数据块进行计算，产生一个唯一指纹。MD5/SHA1

发送给其他人你的信息和摘要,其他人用相同的加密方法得到摘要，最后进行比较摘要是否相同。

MD5(Message Digest algorithm 5，信息摘要算法)

SHA(Secure Hash Algorithm，安全散列算法)

2:单匙密码体制:DES:比较简便高效,密钥简短，加解密速度快，破译极其困难,但其安全性依赖于密匙的安全性。

DES（Data Encryption Standard）是发明最早的最广泛使用的分组对称加密算法。DES算法的入口参数有三个：Key、Data、Mode。其中Key为8个字节共64位，是DES算法的工作密钥；Data也为8个字节64位，是要被加密或被解密的数据；Mode为DES的工作方式，有两种：加密或解密

3:数字签名:就是信息发送者用其私钥对从所传报文中提取出的特征数据（或称数字指纹）进行RSA算法操作，以保证发信人无法抵赖曾发过该信息（即不可抵赖性），同时也确保信息报文在经签名后末被篡改（即完整性）。当信息接收者收到报文后，就可以用发送者的公钥对数字签名进行验证。

代表：DSA

4:非对称密匙密码体制（公匙体系）：加密密匙不同于解密密匙，加密密匙公之于众，谁都可以使用，解密密匙只有解密人自己知道。代表：RSA