**开发常用到的几种加密方式**

一、MD5 加密(散列算法)

1、概念

MD5是一种基于哈希函数的单向加密算法，只能加密、无法解密，它是把一个任意长度的字节串变换成一定长的大整数。请注意我使用了"字节串"而不是"字符串"这个词，是因为这种变换只与字节的值有关，与字符集或编码方式无关。 MD5将任意长度的"字节串"变换成一个128bit的大整数，并且它是一个不可逆的字符串变换算法，换句话说就是，即使你看到源程序和算法描述，也无法将一个MD5的值变换回原始的字符串，从数学原理上说，是因为原始的字符串有无穷多个，这有点象不存在反函数的数学函数。MD5是不可逆的只有加密没有解密。

2、iOS代码加密使用方式如下

NSString \*password = @“密码”;

 const char \*cStr = [password  UTF8String];

 unsigned char result[CC\_MD5\_DIGEST\_LENGTH];

    CC\_MD5(cStr, strlen(cStr), result);

 password =[[NSString stringWithFormat:@"%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X%02X",

             result[0], result[1], result[2], result[3],

             result[4], result[5], result[6], result[7],

             result[8], result[9], result[10], result[11],

             result[12], result[13], result[14], result[15]

             ] lowercaseString];

  单纯的 MD5加密是不安全的，通过第三方网站是有很大可能被暴力破解出来的，因此最好配合 MD5加盐的方式来对密文进行再次处理，即往密文中插入或拼接一个指定的字符串。

盐值加如的代码例子如下

 password = [password stringByAppendingString:salt];

3、加密强度

1）未加盐 ：2颗星

2）加盐：4颗星

二、时间戳/动态密码 的加密

1、实现目标

用户的密码是一定的,但是每次发送给网络的密码都不同.相同的密码相同的加密算法,每次获得的值不同.客户端和服务器端的时间是相同的.

2、原理

  客户端和服务器端依时间为基准采用相同的加密算法

3、实现细节

客户端和服务器端要求时间一致，时间精度越高,越安全

客户端:发送网络请求的时候依当前时间为基准进行加密.

服务器端:以接收到时间为基准进行加密.还要以接收到的时间的前一分钟时间为基准进行加密.

服务器端:判断这两次的密码和客户端发送的密码是否一致。

4、加密强度：5颗星

三、Base64加密(base64 是一种编码方式，只能算是浅加密,是对称加密)

1、概念

Base64编码的思想是：采用64个基本的ASCII码字符对数据进行重新编码。它将需要编码的数据拆分成字节数组，以3个字节为一组，按顺序排列24位数据，再把这24位数据分成4组，即每组6位；再在每组的的最高位前补两个0凑足一个字节，这样就把一个3字节为一组的数据重新编码成了4个字节；当所要编码的数据的字节数不是3的整倍数，也就是说在分组时最后一组不够3个字节，这时在最后一组填充1到2个0字节，并在最后编码完成后在结尾添加1到2个=号。

2、特点：

- 数据加密之后，数据量会变大，变大1/3左右。  
- 可进行反向解密。  
- 编码后有个非常显著的特点，末尾有个=号。

在iOS中Base64加解密。比较简单，容易被破解

3、加密强度：3颗星

三、使用DES加密（对称加密）

数据加密标准算法(Data Encryption Standard)，和BASE64最明显的区别就是有一个公有密钥，该密钥既用于加密、也用于解密，并且要求密钥是一个长度至少大于8位的字符串。使用DES加密、解密的核心是确保工作密钥的安全性。

1. 根据key生成密钥：

2. 加密操作：

3. 为了便于观察生成的加密数据，使用BASE64再次加密：

4. 解密操作：

四、AES加密（对称加密）

1、概念

高级加密标准Advanced Encryption Standard简称：AES，在密码学中又称Rijndael加密法，是美国联邦政府采用的一种区块加密标准。它是一种对称加密算法，这个标准也替代原先的DES标准，已经被多方分析且广为全世界所使用。AES设计有三个密钥长度:128、192、256位，相对而言，AES的128密钥比DES的56密钥强1021倍。AES算法主要包括三个方面：轮变化、圈数和密钥扩展。

2、特点

AES作为新一代的数据加密标准汇聚了强安全性、高性能、高效率、易用和灵活，在软件及硬件上都能快速地加解密且只需要很少的存储资源等优点。

3、加密强度：4颗星

五、RSA加密(非对称加密)

1、概念

RSA是目前最有影响力的公钥加密算法，它能够抵抗到目前为止已知的绝大多数密码攻击，已被ISO推荐为公钥数据加密标准。RSA的公开密钥密码体制就是使用不同的加密密钥与解密密钥，是一种“由已知加密密钥推导出解密密钥在计算上是不可行的”密码体制。通常是先生成一对RSA密钥，其中之一是保密密钥，由用户保存；另一个为公开密钥，可对外公开，甚至可在网络服务器中注册。为提高保密强度，RSA密钥至少为500位长，一般推荐使用1024位，这就使加密的计算量很大。RSA算法是一种非对称密码算法，所谓非对称，就是指该算法需要一对密钥，使用其中一个加密，则需要用另一个才能解密。

RSA算法是非对称加密算法的典型代表，既能加密、又能解密。和对称加密算法比如DES的明显区别在于用于加密、解密的密钥是不同的。使用RSA算法，只要密钥足够长(一般要求1024bit)，加密的信息是不能被破解的。用户通过https协议访问服务器时，就是使用非对称加密算法进行数据的加密、解密操作的。

服务器发送数据给客户端时使用私钥（private key）进行加密，并且使用加密之后的数据和私钥生成数字签名（digital signature）并发送给客户端。客户端接收到服务器发送的数据会使用公钥（public key）对数据来进行解密，并且根据加密数据和公钥验证数字签名的有效性，防止加密数据在传输过程中被第三方进行了修改。

客户端发送数据给服务器时使用公钥进行加密，服务器接收到加密数据之后使用私钥进行解密。

1. 创建密钥对KeyPair：

2. 获取公钥/私钥：

3. 服务器数据使用私钥加密：

4. 用户使用公钥解密：

5. 服务器根据私钥和加密数据生成数字签名：

6. 用户根据公钥、加密数据验证数据是否被修改过：

2、特点  
 - RSA密钥管理的方便，计算量很大速度相对比较慢。  
 - RSA安全性很高，能够抵抗到目前为止已知的绝大多数密码攻击。

3、加密强度：4.5颗星

五、多种加密方式配合加密

利用多种加密方式，按照约定的相同算法进行配合加密解密，可以将安全程度大大提升，但永远没有绝对安全的加密方式。

**加密算法总结**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | MD5 | Base64 | DES | AES | RSA | 时间戳 |
| 优点 |  |  |  |  |  |  |
| 缺点 |  |  |  |  |  |  |
| 应用场景 |  |  |  |  |  |  |