<https://www.cnblogs.com/lianghui66/archive/2013/03/07/2948494.html>

[**对称加密----AES和DES加密、解密**](http://www.cnblogs.com/lianghui66/archive/2013/03/07/2948494.html)

目前主流的加密方式有：（对称加密）AES、DES        （非对称加密）RSA、DSA

调用AES/DES加密算法包最精要的就是下面两句话：

Cipher cipher = Cipher.getInstance("DES/CBC/PKCS5Padding");  
cipher.init(Cipher.ENCRYPT\_MODE, key, zeroIv);

CBC是工作模式，DES一共有电子密码本模式（[ECB](http://www.hudong.com/wiki/ECB)）、加密分组链接模式（[CBC](http://www.hudong.com/wiki/CBC)）、加密反馈模式（[CFB](http://www.hudong.com/wiki/CFB)）和输出反馈模式（[OFB](http://write.blog.csdn.net/postedit)）四种模式，

PKCS5Padding是填充模式，还有其它的填充模式：

然后，cipher.init（)一共有三个参数：Cipher.ENCRYPT\_MODE, key, zeroIv，zeroIv就是初始化向量。

工作模式、填充模式、初始化向量这三种因素一个都不能少。否则，如果你不指定的话，那么就要程序就要调用默认实现。

代码：

1.加密：

例：加密方式： AES128(CBC/PKCS5Padding) + Base64, 私钥：lianghuilonglong,要加密的字符串abcdefg

public String encrypt(){

　　String text = "abcdefg";   //要加密的字符串

　　String key = "lianghuilonglong";　 //私钥   AES固定格式为128/192/256 bits.即：16/24/32bytes。DES固定格式为128bits，即8bytes。

　　String iv   = "aabbccddeeffgghh";　　//初始化向量参数，AES 为16bytes. DES 为8bytes.

　　Key keySpec = new SecretKeySpec(key.getBytes(), "AES");    //两个参数，第一个为私钥字节数组， 第二个为加密方式 AES或者DES

　　IvParameterSpec ivSpec = new IvParameterSpec(iv.getBytes);

　　Cipher cipher = Cipher.getIntance("AES/CBC/PKCS5Padding");　  //实例化加密类，参数为加密方式，要写全

　　cipher.init(Cipher.ENCRYPT\_MODE,  keySpec, ivSpec);　　           //初始化，此方法可以采用三种方式，按服务器要求来添加。（1）无第三个参数（2）第三个参数为SecureRandom random = new SecureRandom();中random对象，随机数。(AES不可采用这种方法)（3）采用此代码中的IVParameterSpec

　　//cipher.init(Cipher.ENCRYPT\_MODE, keySpec);

　　//SecureRandom random = new SecureRandom();

　　//cipher.init(Cipher.ENCRYPT\_MODE, keySpec, random);

　　byte [] b = cipher.doFinal(text.getBytes());　                   //加密操作,返回加密后的字节数组，然后需要编码。主要编解码方式有Base64, HEX, UUE, 　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　　7bit等等。此处看服务器需要什么编码方式

　　String ret = Base64.encode(b);                                       //Base64、HEX等编解码

}

2.解密：

逻辑： 将服务器返回的加密字符串，先用Base64、HEX等解码成byte[]，再用加密时相同的加密方式及key进行解密。加密与解密代码几乎相同。唯一区别为在Cipher类init时，工作模式为Cipher.DECRYPT\_MODE。代码：

//加密方式： AES128(CBC/PKCS5Padding) + Base64, 私钥：lianghuilonglong

public String deCiphering(){

　　String keySpec = "lianghuilonglong";

　　String textDeCipher = "UstyI8JoQOty8egSMFQfig==";   //从服务器返回的加密字符串，需要解密的字符串

　　byte [] byte = Base64.decode(textDeCipher);　　         //先用Base64解码

　　IvParaterSpec ivSpec = new IvParaterSpec("abcdefghabcdefgh".getBytes());

　　Key key = new SecretKeySpec(keySpec.getBytes(), "AES");

　　Cipher cipher = Cipher.getInstance("AES/CBC/PKCS5Padding");

　　cipher.init(Cipher.DECRYPT\_MODE, key, ivSpec);               //与加密时不同MODE:Cipher.DECRYPT\_MODE

　　byte [] ret = cipher.doFinal(byte);

　　return new String(ret, "utf-8");

}