# Java常用加解密算法

## 常用算法介绍：

【Java安全】关于Java中常用加密/解密方法的实现：<https://www.cnblogs.com/tancky/p/6409823.html>

JAVA中常用的加密算法总结：

<https://blog.csdn.net/chenbing81/article/details/51914151>

### base64

### 原理：

Base64的码表只有64个字符， 如果要表达64个字符的话，使用6的bit即可完全表示(2的6次方为64)。

因为Base64的编码只有6个bit即可表示，而正常的字符是使用8个bit表示， 8和6的最小公倍数是24，所以4个Base64字符可以表示3个标准的ascll字符；

如果是字符串转换为Base64码， 会先把对应的字符串转换为ascll码表对应的数字， 然后再把数字转换为2进制， 比如a的ascll码味97， 97的二进制是：01100001， 把8个二进制提取成6个，剩下的2个二进制和后面的二进制继续拼接， 最后再把6个二进制码转换为Base64对于的编码，（当转换到最后， 最后的字符不足3个字符咋办， 如果不足三个字符的话，我们直接在最后添加‘＝’） 以下为具体的解析过程案例：

字符串 a b c

ASCII 97 98 99

8bit 01100001 01100010 01100011

6bit 011000 010110 001001 100011

十进制 24 22 9 35

对应编码 Y W J j

#### 说明：

Base64是网络上最常见的用于传输8Bit字节码的编码方式之一，Base64就是一种基于64个可打印字符来表示二进制数据的方法。

Base64要求把每三个8Bit的字节转换为四个6Bit的字节（3\*8 = 4\*6 = 24），然后把6Bit再添两位高位0，组成四个8Bit的字节，也就是说，转换后的字符串理论上将要比原来的长1/3。

ase64索引表，字符选用了"A-Z、a-z、0-9、+、/" 64个可打印字符

#### 应用：

Base64编码可用于在HTTP环境下传递较长的标识信息。

Mozilla Thunderbird和Evolution用Base64来保密电子邮件密码。

Base64 也会经常用作一个简单的“加密”来保护某些数据，而真正的加密通常都比较繁琐。

垃圾讯息传播者用Base64来避过反垃圾邮件工具，因为那些工具通常都不会翻译Base64的讯息。

在LDIF档案，Base64用作编码字串。

### AES

### RSA

## 1.1 常用加密解密算法

### 相关概念

数据加密算法：

<https://baike.baidu.com/item/%E6%95%B0%E6%8D%AE%E5%8A%A0%E5%AF%86%E7%AE%97%E6%B3%95/3030864>

公钥与私钥：

<http://www.blogjava.net/yxhxj2006/archive/2012/10/15/389547.html>

单向加密 对称加密 非对称加密：

<https://www.cnblogs.com/yx520zhao/p/6658688.html>

数据加密的一些浅谈总结：

<https://blog.csdn.net/maiwc/article/details/51766131>