1. 公钥加密数据，用私钥解密为加密解密；用私钥加密数据，公钥解密为签名或者验证签名。
2. 实际上应用：相互交换公钥，用对方的公钥加密数据，对方用自己的私钥解密数据。
3. 非对称加密算法：RSA（加解密and签名）；DSA只能用于签名；SHA与MD5算法相同，为摘要算法（依据数据内容生成一种固定长度的摘要，这串摘要值与原数据存在对应关系），原数据可以生产摘要，但是摘要不能还原成原数据。实际应用过程中,因为需要加密的数据可能会很大,进行加密费时费力,所以一般都会把原数据先进行摘要,然后对这个摘要值进行加密,将原数据的明文和加密后的摘要值一起传给你.这样你解开加密后的摘要值,再和你得到的数据进行的摘要值对应一下就可以知道数据有没有被修改了,而且,因为私钥只有你有,只有你能解密摘要值,所以别人就算把原数据做了修改,然后生成一个假的摘要给你也是不行的,你这边用密钥也根本解不开。