RSA：

1. 原理

RSA是一种基于大整数分解的加密的非对称加密方式，公钥和私钥是两个大素数（大于100个十进制位）的函数，其中公钥是公开的，从该公钥和密文推断出私钥进而破解出明文的难度等同于分解两个大素数的积。

1. 优点

容易实现密钥管理；安全性较高，经过30多年的使用，只要密钥长度足够长，RSA就能够保证安全性。

1. 缺点

密钥的产生受素数产生技术的限制，因而难以做到一次一密；

随着大整数素因数分解算法的改进和计算机计算能力的提高，需要的密钥长度越来越大，为保证安全性，目前至少需要1024比特以上，使运算代价很高，尤其是速度较慢，比对称密码算法慢几个数量级；

另外，RSA的安全性是否等同于大数分解未能得到理论上的证明。

1. 应用

日常生活中，一些ID卡（例如公交卡）刷卡，支付宝以及一些网银平台支付时都会用到RSA。

更底层的网络技术也有很多RSA的运用，例如利用OpenSSL库对Socket传输进行安全加密时、https利用SSL加密时都会用到RSA。

其中，刷卡和支付时将RSA作为签名技术，而后两种数据传输时的运用利用其对数据加密。签名和加密是RSA主要的作用。

DSA

1. 原理

DSA是基于整数有限域离散对数难题的非对称加密算法。和RSA加密解密过程相反，在DSA数字签名和认证中，发送者使用自己的私钥对文件或消息进行签名，接受者收到消息后使用发送者的公钥来验证签名的真实性。

1. 优点

安全性与RSA相比差不多，密钥长度也相等；（用于数字签名算法时）签名生成速度很快，解密时速度也很快；一个与RSA重要区别在于两个素数公开，这样，当使用别人的p和q时，即使不知道私钥，你也能确认它们是否是随机产生的，或是被人做过手脚，因此比RSA更适合用作签名。

1. 缺点

验证速度很慢，加密时更慢，与RSA同样需要越来越长的密钥以应对计算能力的提高。

1. 应用

DSA更多地用于数字签名和认证，即确认数据、信息来源可靠。支付宝和一些网银支付平台同样使用了DSA技术，https等安全网络协议的证书也有用到DSA。