(1) 一个密码系统包括：明文空间，密文空间，密钥空间，加密算法和解密算法的集合

(2) RSA算法的理论基础为：大整数素因子分解是困难的问题

RSA算法流程：

①选择两个大素数p或q

②计算 $n=p\times q$ 与 $z=(p-1)\times(q-1)$

③选择与z互质的数令其为d

④找到一个e使满足 $e\times d=1 \pmod z$

⑤公开密钥为(e,n)，私有密钥为(d,n)

加密方法：

①将明文划分为k位的块P，对每个数据块，计算 $C=P^e \pmod n$

解密方法：

①对每个密文块C，计算 $P=C^d \pmod n$，P即为密文

(3)

主要区别包括：

①数字签名的基本目的是认证、核准和负责，防欺骗与抵赖✓；消息鉴别为了保证消息的完整性和真实性，但不能处理双方内部的攻击。可处理双方内部的攻击

②~~数字签名所用的是非对称密码体制；消息鉴别所用的是对称密码体制~~

主要

(4) 三重DES需穷举 2^{112} 次穷举搜索，以2000年PPT上对 2^{56} 次方穷举所需22.5小时为基准，从2000年至此一共经历7个18月，不论设此时性能为当时的 2^8 倍，进行 2^{112} 次穷举搜索所需为 2^{48} 个22.5小时，约为 ~~7.23~~ 7×10^{11} 年，目前上仍是计算上安全的。