1. 一个密码系统可以定义为一个5元组，包含：明文空间，密文空间，密钥空间，加密算法集合和解密算法集合

2. 理论基础是数论中的大整数的素因子分解是困难问题，即求两个大素数的乘积在计算机上是很容易实现的，但要将一个大整数分解为两个大素数之积则是困难的。

3. 密钥计算方法

①选择两个大素数p与q ②计算$n=p\times q$和$z=(p-1)\times(q-1)$

③选择一个与z互质的数，令其为d

④找到一个e使满足$e\times d=1 \bmod z$

⑤公钥为(e,n)；私钥为(d,n)

加密方法：

①将明文看成比特串，并将其划分为k位的块P即可，这里k是满足$2^k<n$的最大整数

②对于每个数据块P，计算$C=P^e \bmod n$，C即为P的密文

解密方法：

对于每个密文块C，计算$P=C^d \pmod n$，P即为明文

消息鉴别是为了保障消息的完整性和真实性，而数字签名是表示签名者对文档内容的认可，并产生某种承诺或法律上的效力。

4. 在2000年时，破解DES需要22.5小时
三重DES的复杂度为一重的2^{56}倍，依据
摩尔定律，现在计算机的性能应为2000
年时的2^{13}倍，因此计算时间应为22.5×2^{43}小时，
显然算法仍然安全