HW2

1、一个密码系统包括一个五元组：明文空间、密文空间、密钥空间、加密算法集合、解密算法集合

2、RSA理论基础：数论中大整数的素因子分解是困难问题，~~没有~~算法运行时间可能会相当长，所以RSA算法可行。

3、RSA算法流程：①首先选择两个大素数 p、q

②计算 $n=p\times q$，$z=(p-1)\cdot(q-1)$

③选一个与 z 互素的数，令其为 d

④找 e 使 $e\times d\equiv 1 \pmod z$

⑤公开密钥 (e,n) 私钥 (d,n)

加密时，对明文 P，密文 $C\equiv P^e \pmod n$

解密：$P\equiv C^d \pmod n$

消息鉴别不能处理通信双方内部的相互攻击，而数字签名是解决通信双方内部相互攻击的最好方法。

4、3重DES被破解需 2^{112} 次穷举搜索，而由摩尔定律，平均18个月计算性能翻一倍，就目前最强超算 Summit 约 200000 TFlop/s 的运算速度，仍需上百年才能在可观的时间内完成解密。所以3重DES目前是安全的