试题一（10 分）：密码系统安全性的定义有几种？它们的含义是什么？

答：现有两种定义“安全性”的方法。一种是基于信息论的方法（经典方法）。另一种是基于计算复杂性理论的方法（现代方法）。

基于信息论的定义是用密文中是否蕴含明文的信息作为标准。不严格地说，若密文中不含明文的任何信息，则认为该密码体制是安全的，否则就认为是不安全的。

基于计算复杂性理论的安全性定义则不考虑密文中是否蕴含明文的信息，而是考虑这些信息是否能有效地被提取出来。换句话说，把搭线者提取明文信息的可能性改为搭线者提取明文信息的可行性，这种安全性称为有条件安全性，即搭线者在一定的计算资源条件下，他不能从密文恢复出明文。

试题二(10 分)： 假设 Hill 密码加密使用密钥 $K=\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}$，试对明文 abcd 加密。

答：（a,b）=(0,1)加密后变为（0,1）×$\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}$=(3,7)=(d,h)； 同理（c,d）=(2,3) 加密后变为（2,3）×$\begin{pmatrix}11 & 8\\ 3 & 7\end{pmatrix}$=(31,37)=(5,11)=(F,L)。

所以，明文(abcd)经过 Hill 密码加密后，变为密文（DHFL）。

试题三（10 分）：设有这样一个密码系统，它的明文空间 $P=\{x,y\}$ 的概率分布为 $p_P(x)=1/4,\quad p_P(y)=3/4$；它的密钥空间 $K=\{a,b,c\}$ 的概率分布为 $p_K(a)=1/2,\quad p_K(b)=p_K(c)=1/4$；它的密文空间 $C=\{1,2,3,4\}$，假定该密码系统的加密函数为：$e_a(x)=1, e_a(y)=2; e_b(x)=2, e_b(y)=3; e_c(x)=3, e_c(y)=4$。请计算：

（1）密文空间的概率分布；

（2）明文关于密文的条件分布；

（3）明文空间的熵。

答：（1）密文空间的概率分布为：1/8；7/16；1/4；3/16

（2）明文关于密文的条件分布 $p(m|c)$ 表如下：

m / c	x	y
1	1	0
2	1/7	6/7
3	1/4	3/4
4	0	1

（3）明文空间的熵为：$H(P) = -\frac{1}{4}\log_2\frac{1}{4} - \frac{3}{4}\log_2\frac{3}{4} = 2 - \frac{3}{4}(\log_2 3) \approx 0.81$

试题四（10 分）设 DES 密码中的初始密钥是 K=（$b_0, b_1, \cdots, b_{63}$，），记 DES 加密算法中 16 轮加密过程中所使用的子密钥分别为 $K_1, K_2, \cdots, K_{16}$。请你计算出第一个子密钥 K_1 的数学表达式。

答：先对初始密钥 K=（$b_0, b_1, \cdots, b_{63}$，）进行一个密钥置换 PC-1（见下 PC-1 表 1），将初始密钥的 8 个奇偶校验位剔除掉，而留下真正的 56 比特初始密钥（C_0 D_0）。接着分别对 C_0 及 D_0 进行左一位循环，得到 C_1 与 D_1 ，连成 56 比特数据。再依密钥置换 PC-2（如下 PC-2 表 2）做重排，便可得到子密钥 K_1。

表 1：密钥置换 PC－1

PC－1						
57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

表 2　密钥置换 PC－2

PC－2					
14	17	11	24	1	5
3	28	15	6	21	10
23	19	12	4	26	8
16	7	27	20	13	2
41	52	31	37	47	55
30	40	51	45	33	48
44	49	39	56	34	53
46	42	50	36	29	32

试题五（10 分）设 p 和 q 是两个大于 2 的素数，并且 n=pq。记$\varphi(m)$是比正整数 m 小，但与 m 互素的正整数个数。再设 e 和 d 是两个正整数，分别满足 gcd(e, $\varphi(n)$)=1 ，ed$\equiv$1(mod$\varphi(n)$)。设函数 E(m)和 D（c）分别定义为 E（m）$\equiv m^e$(mod n)和 D(c) $\equiv c^d$(mod n)。请问（1）$\varphi(n)$等于多少？ （2）请证明对于任何正整数 m，都成立恒等式 D（E（m））=m。

答：（1）$\varphi(n)$=(p-1)(q-1)。

（2）其实，只需要证明 RSA 的解密正确性就行了。当（m,n）=1 时，则由欧拉定理可知 $m^{\varphi(n)}\equiv 1(\mathrm{mod}\, n)$。

当(m,n)>1 时，由于 n=pq，故(m,n)必含 p,q 之一。不妨设(m,n)=p，则 m=cp,(1≤c<q),由欧拉定理知 $m^{\varphi(q)}\equiv 1(\mathrm{mod}\, q)$。

因此，对于任何 k，总有 $m^{k(q-1)} \equiv 1 (\mathrm{mod}\, q)$，　$m^{k(p-1)(q-1)} \equiv (1)^{k(p-1)} \equiv 1 (\mathrm{mod}\, q)$，即 $m^{k\varphi(n)} \equiv 1 (\mathrm{mod}\, q)$。于是存在 h(h 是某个整数)满足 $m^{k\varphi(n)}+hq=1$。由假定 m=cp。故 $m= m^{k\varphi(n)+1}+hcpq= m^{k\varphi(n)+1}+hcn$。这就证明了 $m=m^{k\varphi(n)+1} (\mathrm{mod}\, n)$。

因此对于 n 及任何 m（m<n），恒有 $m^{k\varphi(n)+1} \equiv m (\mathrm{mod}\, n)$。所以，D(E（m）)=D(c) $\equiv c^d = m^{ed} = m^{l\varphi(n)+1} = m (\mathrm{mod}\, n)$。命题得证。

试题六（10 分）：（1）请利用著名的 RSA 公钥密码算法设计一个数字签名算法（称为 RSA 签名算法）。（2）由于 RSA 签名算法每次只能对一个固定长度（比如 N 比特）的消息进行签名，为了对任意长度的消息进行签名，有人建议了这样一种处理方法：首先将长消息切割成固定长度 N 比特的数据块，然后用 RSA 签名算法对每个数据块进行签名，最后将这些签名块拼接起来就得到了长消息的签名。请问这种切割处理方法所获得的签名算法安全吗？为什么？

答：（1）RSA 签名算法的系统参数可设为 n=pq,且 p 和 q 是两个大素数，则 M=A=Z_n,定义K={（n,d,p,q,e）}这里 e 和 d 满足 $ed \equiv 1 (\mathrm{mod}\Phi(n))$(Φ()是欧拉函数)。公开密钥 n,d；私有密钥 p,q,e； 签名算法为 $Sig_{K_2}(x)=x^e \mod n$；签名验证算法为 $Ver(x,y)=TRUE \Leftrightarrow x \equiv y^d (\mathrm{mod} n). (x,y) \in Z_n \times Z_n$。更直观地说，用 RSA 解密算法作为签名，用 RSA 的加密作为验证，于是，只有合法用户自己才能签名，而任何人都可以验证签名的真实性。其实，基于任何一个加、解密算法顺序可交换的密码算法都可用于设计一个数字签名算法，只需要以解密做签名，以加密做验证就行了。

（2）切割和拼接处理方法所获得的签名算法不安全。因为，假如 m 和 n 是两个 N 比特的消息，那么，黑客可以通过已知的 m 和 n 的签名 S(m)S(n)，至少获得另一个消息 nm 的合法签名 S(n)S(m)。

试题七（10 分）：（1）请详细叙述 Diffie-Hellman 密钥预分配协议；（2）如果去掉 Diffie-Hellman 密钥预分配协议中的证书（即不存在可信中心），请你给出一种有效的中间人攻击方法，即攻击者截获通信双方通信的内容后可分别冒充通信双方，以获得通信双方协商的密钥。

答：（1）为完整描述 Diffie-Hellman 密钥预分配协议，用 ID（U）表示网络中用户 U 的某些识别信息。每个用户 U 有一个秘密指数 $a_U (0 \le a_U \le p-2)$ 和一个相应的公钥 $b_U = \alpha^{a_U} \bmod p$。

可信中心有一个签名方案，该签名方案的公开验证算法记为 Ver_{TA},秘密签名算法记为 Sig_{TA}。当一个用户 U 入网时，可信中心需给他颁发一个证书：$C(U)=(ID(U),b_U,Sig_{TA}(ID(U),b_U))$。可信中心对证书的签名允许网络中的任何人能验证它所包含的信息。U 和 V 计算共同的密钥 $k_{U,V} = \alpha^{a_U a_V} \bmod p$ 的协议，即，Diffie-Hellman 密钥预分配协议如下：

1）公开一个素数 p 和一个本原元 $\alpha \in Z_P^*$。

2）V 使用他自己的秘密值 a_V 及从 U 的证书中获得的公开值 b_U，计算

$$k_{U,V} = \alpha^{a_U a_V} \bmod p = b_U^{a_V} \bmod p$$

3）U 使用他自己的秘密值 a_U 及从 V 的证书中获得的公开值 b_V，计算 $k_{U,V} = \alpha^{a_U a_V} \bmod p = b_V^{a_U} \bmod p$

（2）如果在上述 Diffie-Hellman 密钥预分配协议中去掉了可信中心和证书，那么，黑客可以按如下步骤分别与 U 和 V 约定合法的密钥，从而，窃听 U 和 V 的全部通信过程：黑客以 V 的身份，与 U 完成预分配协议，获得一个与 U 共享的密钥 A；同时，黑客以 U 的身份，与 V 完成预分配协议，获得一个与 V 共享的密钥 B。当 U 想将消息 M 加密发送给 V 时，U 用 A 做密钥，由于，黑客知道密钥 A，所以，黑客能够解密获得消息 M。然后，黑客再用 B 做密钥对消息 M 加密，并将此密文发给用户 V，用户 V 用 B 解密获得 M。在该中间人过程中，黑客既能够窃听 U 与 V 通信的全部过程，而且，用户 U 与 V 无法感觉到中间人的存在。