第三章

一、填空：

1. 分组密码中的代换是一种从明文空间到密文空间的一一映射，如果明密文的长度均为 n 比特则不同的可逆代换有多少个_____

2. 从易于实现、提高速度和节省软硬件资源的角度看，加解密算法应具有什么样的特性____

3. 一般情况下，一个 n bit 代换结构其密钥量是_____bit

4. 扩散的目的是_____混淆的目的是_____

5. 就代换和置换两类组件而言，采用_____变换能够达到扩散目的，采用_____变换能实现混淆

6. 乘积密码指顺序地执行两个或多个基本密码系统，如果采用相同的基本密码系统，则这样的乘积密码称为_____，其典型结构是_____

7. 在 Feistel 网络结构的密码中，加解密极其相似，加密和解密算法的唯一不同之处在于_____。

8. DES 的密钥长度_____分组长度_____输出密文长度_____加密轮数_____

9. DES 解密时子密钥的产生有两种方式，对于存储空间受限的环境，采用哪种方式更合适_____

10. DES 的初始置换和扩展置换如表所示，则长为 64 比特的明文分组其第 1、9、17、47 个比特在置换后分别位于哪个位置_____，DES 加密某轮的右 32 比特中第 1、28 比特在经过扩展置换后的位置是_____

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

（a）初始置换

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

（b）扩展置换 E

11. DES 密码的 S 盒定义如下表，如果输入是 101011，则输出是_____

		0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
S	**0**	**14**	**4**	**13**	**1**	**2**	**15**	**11**	**8**	**3**	**10**	**6**	**12**	**5**	**9**	**0**	**7**
	1	**0**	**15**	**7**	**4**	**14**	**2**	**13**	**1**	**10**	**6**	**12**	**11**	**9**	**5**	**3**	**8**
	2	**4**	**1**	**14**	**8**	**13**	**6**	**2**	**11**	**15**	**12**	**9**	**7**	**3**	**10**	**5**	**0**
	3	**15**	**12**	**8**	**2**	**4**	**9**	**1**	**7**	**5**	**11**	**3**	**14**	**10**	**0**	**6**	**13**

12. EDE 的密钥长度_____分组长度_____输出密文长度_____加密轮数_____

13. DES 加密每一轮的子密钥的长度是_____，EDE 加密中一共有____个不同的子密钥

14. 在四种攻击中，差分密码分析属于_____ 线性密码分析属于_____

15. 已知一个 3 轮特征: $\alpha_0, \alpha_1, \alpha_2, \alpha_3$，则 3 轮特征概率为_____

α_0	L_0'= 4008000016	R_0'=0400000016	
α_1	L_1'= 0400000016	R_1'=0000000016	p_1=1/4
α_2	L_2'= 0000000016	R_2'=0400000016	p_2=1
α_3	L_3'= 0400000016	R_3'=4008000016	p_3=1/4

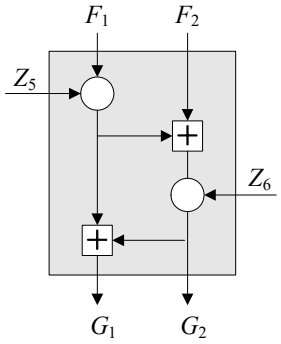
16. CFB-8 的一个比特的密文错误，会导致____个比特的错误传播？在 CFB-12 中，如果一个密文的倒数第二个比特发生了错误，则会导致_____个分组的错误传播。(注意，不包括发生密文错误的分组)

17. 在 IDEA 中，0^2=_____，2^{15}*8=_____，$2^{15}+2^{15}$=_____，2^{15} *2^{15}=_____

18. IDEA 的密钥长度___分组长度____输出密文长度_____加密迭代轮数_____子密钥个数___

19. IDEA 中 8 的乘法逆元是多少_____，加法逆元是多少_____

20. 如图乘加结构，则解密时 Z_5 对应的解密子密钥可表示为_____



MA结构

21. AES 的最小的密钥长度_____分组长度_____输出密文长度_____加密迭代轮数_____

22. 12 轮 AES 算法中，如果密钥长度 k，分组长度为 b，子密钥一共需要_____个比特

23. $(x^4+x+1) \bmod m(x)=x^8+x^4+x^3+x+1$ 的逆元是_____

24. AES 的状态在明文输入时第 n 个字节放在状态阵列的位置(i,j)上，则第 13 个字节所对应的状态阵列的位置(i,j)=_____

二、选择：每一项有 1 个或多个选项是正确的

1. 从古典密码的角度看，分组密码属于_____

A. 单表代换密码　B. 多表代换密码　C. 单表置换密码　D. 多表置换密码

2. 分组密码可以用于实现下述那些功能_____

A. 加密，　B. 产生伪随机数，　C. 产生密钥流序列　D. 产生 MAC　E. 数字签名

3. 实现扩散的方法是_____

A. 置换　B. 代换　C. 先置换再代换　D. 先代换再置换

4. 下面这些密码算法中，属于 Feistel 结构密码的有_____

A. AES　　B. IDEA　　C. RSA　　D. DES

5. 利用 DES 的取反特性进行的攻击，应属于哪一类密码攻击_____

A. 惟密文攻击　B. 已知明文攻击　C. 选择明文攻击　D. 选择密文攻击

6. 下列算法中，哪一个是现行国际分组加密标准_____

A. DES　B. RSA　C.IDEA　D.AES

7. 下列运行模式中，哪一种模式的错误传播最小？_____哪一种模式可将分组密码转换为自同步流密码_____，哪些模式可实现随机读取_____

A. ECB　B.CBC　C.CFB　D.OFB　E. CTR

8. 如上题，AES 状态阵列的第(2,5)位置上的元素对应明文的第_____个字节

A. 22　B. 7　C. 13　D. 10

三、判断：(正确的划"√"，错误的划"×"，以下同)

1. 分组密码用于加密时，其明文和对应密文的长度可以相同，也可以不同。　(　)

2. CFB 运行模式下的分组密码可以等效为一个同步流密码。　(　)

3. OFB 只需要 DES 的加密算法。　(　)

4. 在 AES 的解密算法中，所有密钥都要先进行逆向列混合，再进行轮密钥加　(　)

5. DES 算法是一种多轮迭代密码　(　)

四、简答与计算：

1. 分组密码在设计时，为什么会要求其加解密算法相似？

2. 试描述 Feistel 密码的结构

3.在 Feistel 密码中，如果第 i 轮的输入是 L_{i-1}，R_{i-1}，输出是 L_i，R_i，试用输出表示输入，其中轮函数设为 $F(R_{i-1}, K_i)$

4. 试画出 S 盒的结构，并说明其工作原理，即如何由输入得到输出

5. 已知 DES 满足取反特性，试说明在对 DES 进行选择明文攻击时工作量会减少一半。

6. 一个用单重 DES 加密的密文 C，密钥为 k，如何用 EDE 算法解密？

7. 两个密钥的二重 DES 的中途相遇攻击是如何实现的？

8. 三个密钥的三重 DES 算法结构，如何用该算法解密一重 DES 产生的密文

9. 什么是 ECB 模式，为什么不适合于加密长消息，如果明文长度不是分组的整数倍怎么办?

10. 画出 CBC 模式的逻辑图，并回答其初始向量 IV 为什么要保密?

11. 试分析一下 CBC、CFB、OFB 运行模式的错误传播情况。

12. CFB 和 OFB 哪一个适合有扰信道，为什么？试画出逻辑图

13. 什么是 CTR 模式？为什么可以并行计算和对密文进行随机存取？

14. Rijndael 算法是建立在 GF(2^8)有限域上的，且模多项式为 $m(x)=x^8+x^4+x^3+x+1$，试计算

$(x^6+x^2+x+1)\times(x^4+x+1) \bmod m(x)$，该计算用 x 乘来表示时，试给出计算过程。

15. 系数在 GF(2^8) 的 mod x^4+1 的乘法 $a(x)$ = '01'x^2, $c(x)$='03'x^3+'01'x^2+'01'x+'02' 试计算 $a(x)\times c(x)$。

16. CFB-64 和 CBC 的区别是什么？

17. 某攻击者要破译所截获的某 n 个密文分组，采用穷搜索攻击，试分析以下两种攻击的区别

1) 假设攻击者控制加密机，搜索所有可能的明文并加密，看是否等于截获的密文，从而实现对密文的破译。

2) 已知一些明密文对，搜索所有可能的密钥，然后再用该密钥对密文解密。

18. 以 DES 为例，试分析迭代密码中基本函数的子密钥相同和不同的区别。

五、证明题：

1. 已知 DES 满足取反特性，试证 EDE、3 个密钥的 3DES 都具有取反特性。

2. 试说明 AES 的轮结构中行移位和字节代换的顺序可以互换。

3. 试证明：在 Feistel 结构密码中解密过程第 1 轮的输出等于加密过程最后一轮输入左右两半交换值。

六、综合题

某人要做一个密码芯片，该芯片要实现以下功能：对数据流加密、MAC 认证、产生随机数。为节省硬件资源，如果仅有一重及多重 DES 可用，试分析分别采用何种模式、标准或结构能够实现这些功能