2018091618008 袁昊男

一、1. 电子密码本模式、密码分组链接模式、密码反馈模式、计数器模式

2. 密码编码学、密码分析学

3. 明文、密文

4. 2^n-1

5. 128、192、256

6. 一次一密

7. 扩散、混淆

8. 时间复杂度、空间复杂度.

9. 存储器、反馈函数

10. $p(x)$为本原多项式

二、1. C 2. A 3. D 4. A 5. B 6. C 7. B 8. B

9. C 10. B

三、1. 攻击方式：(1)唯密文攻击：密码分析者只用密文进行密码分析的方法；
(2)已知明文攻击：利用大量互相对应的明文和密文进行密码分析的方法
(3)选择明文攻击：选择特定明文和对应密文进行密码分析的方法；
(4)选择密文攻击：选择特定密文和对应明文进行密码分析的方法；

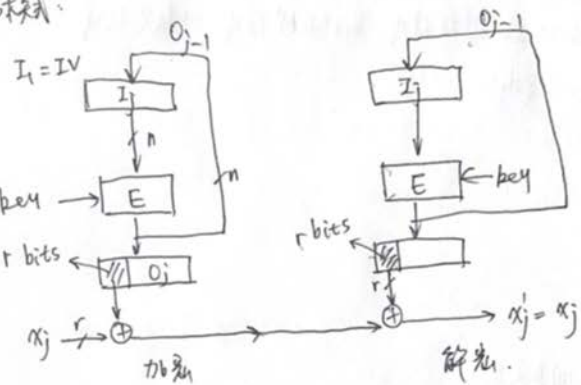
Kerckhoffs原则：加密算法应建立在算法公开不影响明文和密钥安全的前提上，即：密码算法的安全性仅依赖于对密钥的保密。

2. (1) $C_1=1$, $C_2=0$, $C_3=0$, $C_4=1$, $p(x)=1+x+x^4$

(2) 1101011001000011110101 周期为5

(3) 0in1游程：2个；0in2游程：1个；0in3游程：1个.
1in1游程：2个；1in2游程：1个；1in4游程：1个

3. OFB模式：



特点：(1)相同明文，利用CBC及CFB一样，改变IV同样会导致相同的明文输入得到不同的加密输出。

(2)延续传输性：密钥流是独立于明文的

(3)错误传播：有一个或多个比特错误出现在一密文字符会影响该字符的解密，密文字符的某比特位置出错将致使还原明文的相应位置也出错。

(4)错误恢复：OFB模式能从密文比特错误中得以恢复，但在丢失密文比特后无法实现再同步，这是因为丢失密文比特会破坏密钥流的移排。

四、1. HELP → (7,4,11,15) $\xrightarrow[c \equiv 19m+7 \bmod 26]{\text{加密}}$ (10,5,8,6)，即：KFIG.

解密：$m \equiv 19^{-1}(c-7) \bmod 26 \equiv 11(c-7) \bmod 26 \equiv 11c+1 \pmod{26}$

c. KFIG → (10,5,8,6) $\xrightarrow[m \equiv 11c+1 \bmod 26]{\text{解密}}$ (7,4,11,15)，即 HELP.

2.

n	d_n	f_n	L_n	m	f_m
0	1	1	0		
1	0	$1+x$	1		
2	1	$1+x$	1	0	1
3	0	$1+x+x^2$	2		
4	1	$1+x+x^2$	2	2	$1+x$
5	1	$1+x+x^3$	3	4	$1+x+x^2$
6	1	$1+x^2$	3	4	$1+x+x^2$
7		$1+x^3+x^4$	4		

11011

∴线性综合解为 $\langle 1+x^3+x^4, 4\rangle$

3、 $m(x) = x^8 + x^6 + x^5 + x + 1$，即'163'

计算 xtime(b) 公式：若 $b_7 = 0$，则 xtime(b) = 将 b 左移一位，右边补 0

若 $b_7 = 1$，则 xtime(b) = 将 b 左移一位(右补 0)后与

'63'(01100011)做异或运算.

'55'(01010101)，即为 $1 + x^2 + x^4 + x^6$

∴ '66'·'55' = '66' ⊕ '66'·x^2 ⊕ '66'·x^4 ⊕ '66'·x^6.

x '66'·'02' = xtime(66) = 11010110，即'D6'

x^2 '66'·'04' = xtime(D6) = 10001111，即'CF'

x^3 '66'·'08' = xtime(CF) = 11111101，即'FD'

x^4 '66'·'10' = xtime(FD) = 10011001，即'99'

x^5 '66'·'20' = xtime(99) = 01010001，即'51'

x^6 '66'·'40' = xtime(51) = 10100010

∴ '66'·'55' = 01101011 ⊕ 11001111 ⊕ 10011001 ⊕ 10100010

= 10011111，即'9F'