2013-2014学年度春季学期密码学及安全计算期末试题

院系：_____ 班级：_____ 姓名：_____ 学号：_____

§1 古典密码

1. (5分)请用凯撒密码加密以下明文：

$$CRYPTOLOGY$$

2. (5分)请以上题中的明文为密钥，用Playfair密码加密以下明文：

$$ILOVETHU$$

3. (5分)Hill密码的密钥为矩阵$\mathbf{K}$：

$$\mathbf{K} = \begin{pmatrix} 7 & 9 \\ 17 & 16 \end{pmatrix}$$

请求出$\mathbf{K}$的逆矩阵$\mathbf{K}^{-1}$并解密以下密文：

$$NKUSTS$$

4. (5分)用维吉尼亚密码加密明文得到密文如下：

$$FHXTGDEMOWNEMAWD$$

计算密钥长度$m = 4$时的重合指数。

5. (5分)用密钥：

$$MATHS$$

对上题的密文进行解密。

§2 编码与信息论

6. (10分)假设随机变量$\mathbf{X} = \{a, b, c, d, e\}$有概率分布：$Pr[a] = 0.27$, $Pr[b] = 0.12$, $Pr[c] = 0.13$, $Pr[d] = 0.15$, $Pr[e] = 0.33$。

   (a) 计算随机变量$\mathbf{X}$的熵值$H(\mathbf{X})$;

   (b) 使用Huffman算法找出无前缀的最佳编码（概率较小的元素赋值为0）。

§3 分组密码

7. (5分) AES密码算法用8次本原多项式$x^8+x^4+x^3+x+1$定义了有限域$\mathbb{F}_(2^8)$上的乘法运算运算($\otimes$)，即：

$$\mathbb{F}_(2^8) = \mathbb{Z}_2[x]/(x^8+x^4+x^3+x+1)$$

设$a, b \in \mathbb{F}_(2^8)$，其中$a = 0x5$, $b = 0x83$($0x$意思是十六进制表示)，求$a \otimes b$并用十六进制数表示。

8. (10分)设$DES(x, \mathbf{K})$表示使用DES密码在密钥$\mathbf{K}$下对明文x进行加密，假定$y = DES(x, \mathbf{K})$，$y' = DES(c(x), c(\mathbf{K}))$，其中$c(\cdot)$表示对其自变量按比特位取反。试证明$y' = c(y)$(即如果把明文和密钥都按照比特位取反，则密文同样是按比特位取反)

9. (10分)轻量级密码算法SEA采用3比特的S盒，即：

$\mathbf{x} = (x_2, x_1, x_0)$	0	1	2	3	4	5	6	7
$S(\mathbf{x}) = (y_2, y_1, y_0)$	0	5	6	7	4	3	1	2

请将y_0（即最低比特位）表示成x_0, x_1, x_2的多项式的形式（即$y_0 = p(x_0, x_1, x_2) \in \mathbb{F}_2[x_0, x_1, x_2]$）

10. (10分)分组密码的五种工作模式中，CBC相对于EBC模式的优势是什么？简述CBC模式如何同时实现加密和完整性认证两个目的。

§4 Hash函数

11. (5分)一个合格的Hash函数应该具备哪些主要性质？

12. (5分)消息认证码主要分为哪几类？请各举一例。

§5 公钥密码

13. (10分)在RSA密码体制中，设两个大素数分别为$p = 13, q = 7$, 公钥$a = 5$,私钥$b = 29$。使用该RSA密码体制：

    (a) 加密明文64;

    (b) 解密密文61。

14. (10分)用ElGamel算法参数设置如下：

    - 私钥a;

- 公开部分：为大素数p，生成元α，公钥$\beta = \alpha^a$；

设计一种基于ElGamel算法的签名和验证方案，使得该方案能够有效抵御中间人攻击（简述签名过程、验证过程，以及哪一步操作可以抵御中间人攻击）。