《离散数学二》第三次作业

1. ISBN-13 有 13 位数字 a1a2…a13，其中校验位 a13 由同余式 (a1 + a3 +…+ a13) + 3(a2 + a4 +…+ a12) ≡ 0 (mod 10) 确定。下列两个ISBN-13是否为有效ISBN-13？(a) 978-0-45424-521-1；（b）978-3-16-148410-0 **(10 分)**

2. 利用仿射加密函数 F(x)=5x+8 mod 26 对字符串“HELLO”进行加密，并对该密文进行解密，要求写出具体过程（10 分）

3. 使用五个字母为一组的块，以及基于排列 {1, 2, 3, 4, 5} 的置换密码(又名转置密码)，其中 $\sigma(1) = 3, \sigma(2) = 5, \sigma(3) = 1, \sigma(4) = 2, \sigma(5) = 4$，来加密消息 “GRIZZLY BEARS”；再根据该转置函数的逆还原成明文。[如果最后一个块不足五个字母，则使用字母 “X” 来填充]。（20 分）

4. 利用 RSA 密码系统进行加解密，其中公钥(n,e)=(391,3)；(1)请给出私钥 d；(2)对字符串 HELLO 中各个字符进行加密；(3)对加密后的密文进行解密，从而恢复出明文 HELLO。[说明：每个字符对应 Z_{26} 里一个数字，譬如 A 对应 0，C 对应 2.] **(20 分)**

5. 描述 Alice 和 Bob 使用 Diffie-Hellman 密钥交换协议生成共享密钥时所遵循的步骤。假设他们使用素数 p = 101，并取 a = 2，

(1)在 Z_{101} 中选择 3,6,9,100 四个数来验证 a=2 是 模 101 的原根；

（2） Alice 选择私钥 k1 = 7，而 Bob 选择私钥 k2 = 9，计算他们各自使用的公钥和共享密钥. （20 分）

6. 设 Alice 和 Bob 利用 RSA 公钥密码体系进行通信，Alice 的公钥: N_A=21, e_A=5；Bob 的公钥 N_B=39,e_B=7，(1)分别计算 Alice 和 Bob 的私钥 d_A 和 d_B；（2）Alice 想要向 Bob 发送数字消息 11，以便他知道她发送了该消息，并且只有 Bob 可以阅读该消息。假设她签署了该消息，然后使用 Bob 的公钥对其进行加密，她应该向 Bob 发送什么？（3）给出 Bob 解密 Alice 所发送的密文过程。**(20 分)**