《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. (1) 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；（2）请证明仿射加密函数F(x)=ax+b mod 26为双射函数，当且仅当gcd(a, 26)=1，这里a,b均为整数. [说明：每个字符对应Z26里一个数字，譬如A对应0，C对应2.]**（20分）**
3. 使用五个字母为一组的块，以及基于排列 {1, 2, 3, 4, 5} 的转置密码，其中 𝜎(1) = 3, 𝜎(2) = 5, 𝜎(3) = 1, 𝜎(4) = 2, 𝜎(5) = 4，来加密消息 “GRIZZLY BEARS”；再根据该转置函数的逆还原成明文。[说：如果最后一个块不足五个字母，则使用字母 “X” 来填充]。**（10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Z26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Z101中选择 3,6,9,100四个数来验证a=2是 模101 的原根，即是找到相应的x，使得2^x mod 101分别等于3,6,9，和10；（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: NA=21, eA=5；Bob的公钥NB=39,eB=7，(1)分别计算Alice和Bob的私钥dA和dB；（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)**