离散数学二，第三次作业

1.参考答案：

（**a**）(9 + 8 + 4 + 4 + 4 + 2 + 1) + 3(7 + 0 + 5 + 2 + 5 + 1) mod 10 = 2; 无效

(b) (9 + 8 + 1 + 1 + 8 + 1 + 0) + 3(7 + 3 + 6 + 4 + 4 + 0) mod 10 = 0; 有效

2.参考答案：

(1) 先将每个字母转换为数字（H=7, E=4, L=11, L=11, O=14）。
加密：应用加密公式 $F(x) = (5x + 8) \bmod 26$ 对每个字母进行加密。
以下是加密步骤：
对于 H (7): $F(7) = (5*7 + 8) \bmod 26 = 43 \bmod 26 = 17$，对应字母 R。
对于 E (4): $F(4) = (5*4 + 8) \bmod 26 = 28 \bmod 26 = 2$，对应字母 C。
对于 L (11): $F(11) = (5*11 + 8) \bmod 26 = 63 \bmod 26 = 11$，对应字母 L（这里加密后还是 L）。
对于 O (14): $F(14)= (5*14 + 8) \bmod 26 = 78 \bmod 26 = 0$，对应字母 A。
因此，明文“HELLO”被加密为“RCLLA”。
解密：解密需要找到加密函数的逆函数。为了找到逆元，我们需要一个与 a 互质且小于 26 的数 $a^{-1} \bmod 26 = 21$，因为 $(5 * 21) \bmod 26 = 105 \bmod 26 = 1$。
解密公式为 $x = a^{-1} * (y - b) \bmod 26$。
以下是解密步骤：
对于 R (17): $x = 21 * (17 - 8) \bmod 26 = 21 * 9 \bmod 26 = 189 \bmod 26 = 7$，对应字母 H。
对于 C (2): $x = 21 * (2 - 8) \bmod 26 = 21 * (-6) \bmod 26 = -126 \bmod 26 = 4$，对应字母 E。
对于 L (11): $x = 21 * (11 - 8) \bmod 26 = 21 * 3 \bmod 26 = 63 \bmod 26 = 11$，对应字母 L。
对于 A (0): $x = 21 * (0 - 8) \bmod 26 = 21 * (-8) \bmod 26 = -168 \bmod 26 = 14$，对应字母 O。
因此，密文“RCLLA”被解密为原始的明文“HELLO”。

3.参考答案：

分成 3 个块，GRIZZ LYBEA RSXXX，则每个块中字符转置后为 IZGZR BELAY XXRXS;

转置函数的逆为：$\sigma^{-1}(1) = 3, \sigma^{-1}(2) = 4, \sigma^{-1}(3) = 1, \sigma^{-1}(4) = 5, \sigma^{-1}(5) = 2$，则密文 IZGZR BELAY XXRXS 解密后为：GRIZZ LYBEA

RSXXX.

4. 参考答案：

(1)n=391=17*23,则φ(391)=16*22=352；所以 $d=3^{-1} \bmod 352=235$；

(2) 先将每个字母转换为数字（H=7, E=4, L=11, L=11, O=14），则：

对于 H (7): 7^3 mod 391=343;

对于 E (4): 4^3 mod 391=64;

对于 L (11): 11^3 mod 391=158

对于 O (14): 14^3 mod 391=7

(3) 343 对应的明文为：343^235 mod 391=7;

64 对应的明文为：64^235 mod 391=4

158 对应的明文为：158^235 mod 391=11

7 对应的明文为：7^235 mod 391=14

5.参考答案：

（1）$2^3 \bmod 101=8$， $2^6 \bmod 101=64$， $2^9 \bmod 101=7$ ，

$2^{100} \bmod 101=1$，a=2 是模 101 的原根。

（2）90

6.参考答案：

（1）$d_A=5^{-1} \bmod \phi(21)= 5^{-1} \bmod 12=5$

$d_B=7^{-1} \bmod \phi(39)= 7$

(2) Alice 向 Bob 发送的明文 11 并加了其签名的密文为:

$E_B(D_A(11))= 2^7 \bmod 39=11$

(3)Bob 的解密过程为:

$E_A(D_B(11))= 2^7 \bmod 39=11$