| 日期 | 科目 | 班级 | 姓名 | 学号 |
| --- | --- | --- | --- | --- |
| 2022 年 9 月 20 日 | 数学建模 | 强基数学 002 | 吴天阳 | 2204210460 |

**题目 1.** 取 $A=\begin{bmatrix}1 & 2\\ 0 & 5\end{bmatrix}$，用 $A$ 加密 `meet`，求其逆矩阵对其解密.

**解答.** 将字符与数字进行对应：$a:1, b:2, \cdots, y:25, z:0$，原文矩阵为 $P=\begin{bmatrix}13 & 5\\ 5 & 20\end{bmatrix}$，在模 26 意义下，密文矩阵为 $Q=AP=\begin{bmatrix}23 & 19\\ 25 & 22\end{bmatrix}$，于是对应的密文为 `wysv`. 在模 26 意义下，$A^{-1}=\begin{bmatrix}1 & 10\\ 0 & 21\end{bmatrix}$，通过计算可得 $A^{-1}Q=P$，从而实现解密.

**题目 2.** 有密文如下：`goqbxcbuglosnfal`；根据英文的行文习惯以及获取密码的途径和背景，猜测是两个字母为一组的希尔密码，前四个明文字母是 `dear`，试破解这段密文.

**解答.** 密文前四个字母对应的密文矩阵为 $Q=\begin{bmatrix}7 & 17\\ 15 & 2\end{bmatrix}$，在模 26 下其逆矩阵为 $Q^{-1}=\begin{bmatrix}22 & 21\\ 17 & 25\end{bmatrix}$，密文对应的明文矩阵为 $P=\begin{bmatrix}4 & 1\\ 5 & 18\end{bmatrix}$，则可得 $A^{-1}=PQ^{-1}=\begin{bmatrix}1 & 5\\ 0 & 9\end{bmatrix}$.

密文 `goqbxcbuglosnfal` 对应的密文矩阵为

$$Q=\begin{bmatrix}7 & 17 & 24 & 2 & 7 & 15 & 14 & 1\\ 15 & 2 & 3 & 21 & 12 & 19 & 6 & 12\end{bmatrix}$$

通过加密矩阵可得

$$P=A^{-1}Q=\begin{bmatrix}4 & 1 & 13 & 3 & 15 & 6 & 18 & 9\\ 5 & 18 & 1 & 7 & 4 & 15 & 2 & 4\end{bmatrix}$$

破解得到的明文为 `dearmacgodforbid`.