

- 1、已知密文为 **SG6T20FGB220V**，其中加密矩阵为 A，大写字母及数字的值表如下，试求出明文。（程序取名为 hw41.m）

注：解密矩阵也要用程序实现，不能手算！

$$A = \begin{pmatrix} 1 & 6 \\ 0 & 7 \end{pmatrix}$$

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

1	2	3	4	5	6	7	8	9	0
27	28	29	30	31	32	33	34	35	0

- 2、利用 Hill2 密码体制的原理，设计 Hill4 密码体制的加密、解密过程。

- (1) 设给定的大写英文字母和空格的表值如下（乱序），试编程实现字符与表值之间的转换；（程序取名为 hw42.m）

A	B	C	D	E	F	G	H	I	J	K	L	M
5	23	2	20	10	15	8	4	18	25	0	16	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z	空格
7	3	1	19	6	12	24	21	17	14	22	11	9	26

- (2) 编程验证下面的矩阵能否作为 Hill4 的加密矩阵；（程序取名为 hw43.m）

$$A = \begin{bmatrix} 8 & 6 & 9 & 5 \\ 6 & 9 & 5 & 10 \\ 5 & 8 & 4 & 9 \\ 10 & 6 & 11 & 4 \end{bmatrix}$$

- (3) 设明文为 **“HILL CRYPTOGRAPHIC SYSTEM IS TRADITIONAL”**，利用上面的表值与加密矩阵给此明文加密，并将得到的密文解密。（程序取名为 hw44.m）