

1. To design a Hill cipher, remove spaces, comma, period etc. from the message to be encoded and partitioned it into groups of  $n$  letters (add extra letters to end if necessary). Assign a number to each letter of the alphabet as given in the table below and each group is formed into a column matrix  $P$ .

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

The matrix  $P$  is then multiplied by an  $n \times n$  invertible encryption matrix  $K$  and the resulting numbers translated back into letters to create an encrypted message  $C = KP$ .

The recipient of this encrypted message finds the plaintext  $P = K^{-1} C$ .

- (a) Implement encryption and decryption of the Hill Cipher on variable length (300 or more) plain text and ciphertext. The key could also be of variable length.
- (b) Write program to analyze the ciphertext, knowing  $n^2$  plaintext and corresponding  $n^2$  cipher text characters. Use Index of coincidence to check whether assumed key size is correct or not. Assume that key size i.e.  $n$  is not too big may be max 10.

Programming language: C/C++ / Python/Matlab.

Deadline: 9<sup>th</sup> September 2021, 11.59 PM