Practical Session 1

The Bifid cipher

The Bifid cipher was created in about 1901 by a French cryptographer, Félix Delastalle. Although it has never been used for military or any other "serious" purpose, it has a very elegant design, is easy to implement, and quite hard to break given its simplicity.
The key for this cipher is any permutation of the alphabet (except for the letter J). One way to remember a key is to choose a word with no repeating letters such as "ENCRYPT" to start the permutation, and finish with the remaining letters. This permutation is placed in a 5 x 5 array called the tableau.
This produces:

	0	1	2	3	4
0	E	N	C	R	Y
1	P	T	A	B	D
2	F	G	H	I	K
3	L	M	O	Q	S
4	U	V	W	X	Z

For this tableau, A has indices 1 and 2; while X has indices 4 and 3.
To use the Bifid cipher, encode the message using the indices from the tableau. So that, for example, the message “MEET ME ON FRIDAY” would be encoded as

M	E	E	T		M	E		O	N		F	R	I	D	A	Y
3	0	0	1		3	0		3	0		2	0	2	1	1	0
1	0	0	1		1	0		2	1		0	3	3	4	2	4

The indices are then read off row by row:

3 0 0 1 3 0 3 0 2 0 2 1 1 0 1 0 0 1 1 0 2 1 0 3 3 4 2 4

These indices then are grouped back into pairs and turned into letters by using the original tableau:

30	01	30	30	20	21	10	10	01	10	21	03	34	24
L	N	L	L	F	G	P	P	N	P	G	R	S	K

The ciphertext is thus “LNLLFGPPNPGRSK”.

1. Describe step by step how you can decrypt a message using the Bifid cipher.
2. Use the Bifid cipher with the tableau as given to
    a. encrypt BRING ALL YOUR MONEY
    b. decrypt PDRRNGBENOPNIAGGF
3. Create the pseudo-code to implement the Bifid cipher. This including message encryption and decryption.
4. After that, implement your pseudo-code in the programming language you decide and uploaded to the corresponding assignment in Alphagrader.

NOTE: The submission of this file with the corresponding answers is individual.