

BIFID

In classical cryptography, the bifid cipher is a cipher which combines the Polybius square with transposition, and uses fractionation to achieve diffusion. It was invented around 1901 by Felix Delastelle.

The Bifid cipher is a type of matrix, or columnar transposition, cipher. Start by creating a 5 by 5 matrix of letters, with the rows and columns labeled 1 to 5:

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I	J
3	K	L	M	N	O
4	P	Q	R	S	T
5	U	V	W	X	YZ

To start, find the value of each letter by reading the row and the column values. The two numbers are then written vertically on a piece of paper below the plain letter. All the plain letters within the secret message are written next to one another as seen below:

Plain Message: S E N D R E I N F O R C E M E N T
Row Value: 4 1 3 1 4 1 4 3 2 3 4 1 1 3 1 3 4
Column Value: 4 5 4 4 3 5 4 4 1 5 3 3 5 3 5 4 5

Notice how the letter "S" has the value of 44. "E" is 15 since it is found in row 1, column 5. Y and Z share the position of (5,5) in the matrix above. After the message has been written out, with row and column values written as shown above, you rewrite the message from left to right, combing numbers into groups of 2.

41 31 41 43 23 41 13 13 44 54 43 54 41 53 35 35 45

The last step is to take each group of numbers, such as 41 and 31 in the beginning of the line above, and find the corresponding cipher values in the same matrix above. 41 is row 4, column 1, the letter "P."

41 31 41 43 23 41 13 13 44 54 43 54 41 53 35 35 45
P K P R H P C C S X R X P W O O T