SYMMETRY OF POSITION

Useful for cryptanalyzing polyalphabetic ciphers such as Mixed Vigenère, in which each cipher alphabet is a cyclic shift of the others. The idea is that, if the relative position of a pair of characters is known in one row, determination of either in another row allows one to fix the position of the other character in that row.

Example 0.1. Suppose that as the result of an analysis based upon considerations of frequency, we have assumed the following values in a given cryptogram:

Plain	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
Cipher 1					G										Y					V						
Cipner 2					N										G					P						
Cipher 3					L										B					I						
Cipher 4					W										I					Q						

Note that the letter G is common to cipher alphabets 1 and 2. In alphabet 2, we note that N occupies the 10th position to the left of G, and the letter P occupies the 5th position to the right of G. We may therefore place these letters, N and P, in their proper positions in alphabet 1, the letter N being placed 10 letters before G, and the letter P, 5 letters after G. Thus:

Plain	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
Cipher 1					G					P					Y					V	N					
Cipher 2					N										G					P						
Cipher 3					L										B					I						
Cipher 4					W										I					Q						

Using the same G, we can also map Y and V into alphabet 2:

Plain	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
Cipher 1					G					P					Y					V	N					
Cipher 2				V	N										G					P					Y	
Cipher 3					L										B					I						
Cipher 4					W										I					Q						

Similarly, we can use symmetry of position to compare alphabets 3 and 4:

Plain	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
Cipher 1					G					P					Y					V	N					
Cipher 2				V	N										G					P					Y	
Cipher 3					L					W					B					I					Q	
Cipher 4					W					B					I					Q						L

Use the new information to fill in more parts of the plaintext, and try to guess at new words. Then, go back to the table and use symmetry of position, etc.