GRONSFELD

One of the simplest polyalphabetic substitution ciphers is Gronsfeld's system. Gaspar Schott, a German 17-century cryptographer, tells that he was taught this cipher during a trip between Mainz and Frankfurt by count Gronsfeld, hence the name.
Gronsfeld's system uses a numeric key - usually quite short - e.g. 7341, and this key is repeated, one figure at a time, above the individual letters of the plaintext, like this:

Key:	7	3	4	1	7	3	4	1	7
Text:	G	R	O	N	S	F	E	L	D

To encrypt, one simply count forwards in the alphabet from the letter to be encrypted, the number of steps given by the keyfigure above, the resulting letter being the crypto. If one happens to reach the last letter of the alphabet, still having remaining steps to count, one begins from the beginning of the alphabet. It helps to think of the alphabet as a ring of letters, instead of a row.

This is how the example from above will look like:

Key:	7	3	4	1	7	3	4	1	7
Text:	G	R	O	N	S	F	E	L	D
Crypto:	N	U	S	O	Z	I	I	M	K

Decryption is the reverse process. One writes out the keyfigures above the letters of the cryptogram and counts backwards in the alphabet instead, to reach the plaintext.

Gronsfeld's system can be made more secure (the original system isn't very safe, even with keys as long as the number of letters in the plaintext) against enemy decryption by using an *unordered alphabet* instead of the normal sequence.

Since there are numerous ways to design an unordered alphabet, I will show but one method. Using the key (or, preferably, another key of one's own choosing) from the example above, the following table is constructed:

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

Writing the letters out, row by row, and starting with the row having the lowest keyfigure gives the following unordered sequence:

DHLPTXBFJNRVZCGKOSWAEIMQUY

The encryption example from above will, when counting in this unordered alphabet, look like this:

Key:	7	3	4	1	7	3	4	1	7
Text:	G	R	O	N	S	F	E	L	D
Crypto:	I	C	E	R	U	R	U	P	F

[Excerpt from "Polyalphabetic substitution" by Torbjörn Andersson]