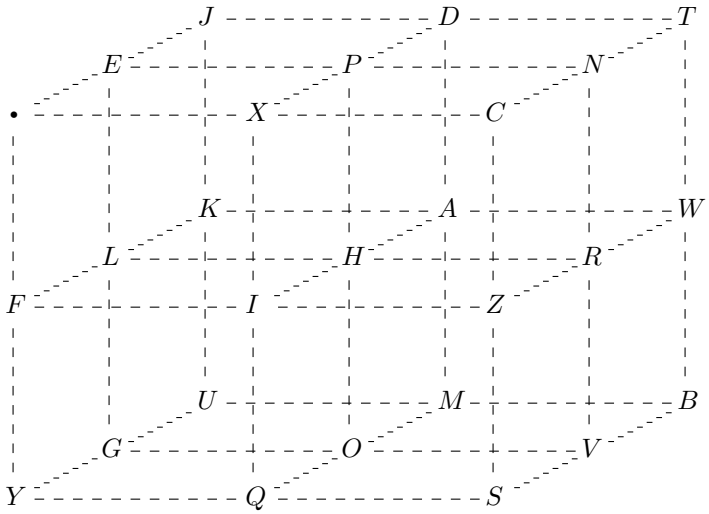
**Trifid Ciphers**

Trifid ciphers are examples of *combination ciphers:* The encryption process consists of a sequence of several different techniques. In this case substitution followed by fractionation and transposition are used in the encryption. The trifid cipher was invented by amateur cryptographer Félix Delastelle, ca. 1900.

The encryption key for a trifid cipher consists of a positive integer (the *period*) and a $3\times3\times3$ array containing all of the distinct letters of the English alphabet plus one additional character. Typically, the additional character in the array is a symbol, such as a dot. The arrangement of the characters in the key array can be chosen at random.




Suppose we want to encrypt the message "trick or treat" using a trifid cipher with encryption key consisting of period 4 and the above array.

*i.* Imagine the coordinate axes are arranged so that the near lower left corner of the array has coordinates (1,1,1), the positive $x$-axis is to the right, the positive $y$-axis points away from the reader, and the positive $z$-axis is upward. Represent the letters in our message "trick or treat" with their coordinates in the encryption array:

333 322 212 313 132 221 322 333 322 123 232 333

*ii.* Now arrange these coordinates in columns:

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 3 | 3 | 2 | 3 | 1 | 2 | 3 | 3 | 3 | 1 | 2 | 3 |
| 3 | 2 | 1 | 1 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 3 |
| 3 | 2 | 2 | 3 | 2 | 1 | 2 | 3 | 2 | 3 | 2 | 3 |

and separate the columns into groups of 4 (the period is 4).

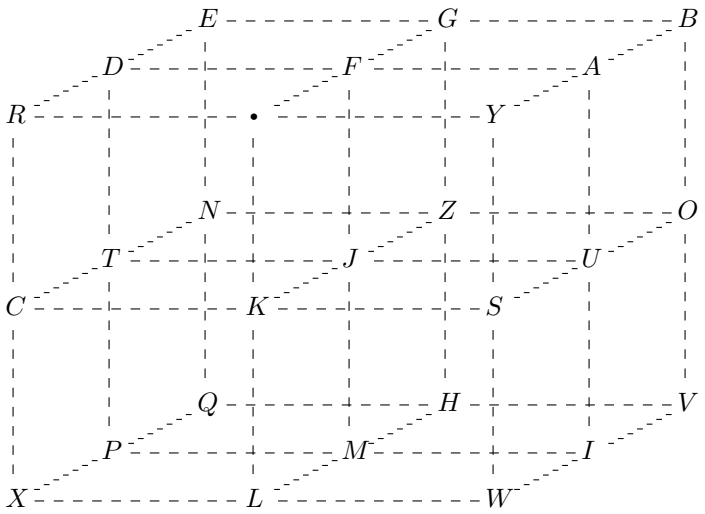
*iii.* Concatenate the rows of each group successively: 332332113223123332232123312322332323

*iv.* Finally, taking the digits in the string from step *iii* in groups of 3, use the key array to replace each group with its corresponding character to obtain the ciphertext: WW•PEWAEZRWN

Notice that at the end of step *i*, essentially we have the result of a substitution cipher. However, instead of replacing each plaintext character with a single symbol, it is replaced by 3 digits. In the subsequent steps

these digits are separated and mixed with the digits obtained from other plaintext characters (fractionation and transposition).

For practice, try encrypting the plaintext "costume party" using a trifid cipher with period 6 and the encryption array below, (this should result in the ciphertext ENQJJMRRUPYA).




The following ciphertext was produced using a trifid cipher with period 4 and the above encryption array.

AQ•N•XJZVCUAEDHKXFZVYJRF

See if you can decrypt it.

Separately, substitution and transposition ciphers have obvious vulnerabilities. When both are combined with fractionation, as in the trifid cipher, these vulnerabilities are lessened considerably. However, cryptanalysis of the trifid cipher is sufficiently effective so that its use for sensitive messages is ill-advised.

Even though implementation is easy, (it can be done with pencil and paper), and security is better than many other pencil and paper ciphers, practical use of the trifid cipher has been infrequent. It is significant as a link between the classical and the modern: Many present-day encryption procedures, (e.g. AES), consist of more complicated, machine-implemented combinations of substitution, fractionation, and transposition.