VIGENÈRE

The most common polyalphabetic substitution cipher is the Vigenere or, as it is sometimes referred to, Tritheim's system. Blaise de Vigenère actually produced a more sophisticated autokey cipher, but through an accident of history his name has become attached to this weaker cipher.

It uses a table, usually containing 26 by 26 cells (one 18-century Swedish table uses 22 by 22 cells, and a 19-century one - also Swedish - has 56 by 56 cells, but it was probably to cumbersome to use) containing the letters of the alphabet in the following fashion (The Vigenere Table):

The cipher text is formed by first writing the key underneath the plain text. In the following example we will use the plain text "encryption rocks" and the key "alabaster".

```
plaintext      encryption rocks
key(repeated) alabastera labas
```

Now, we will demonstrate how to form the cipher text. First, find the letter of the plain text on the top of the table, then drop down to the

letter row of the key letter. The first letter from the table is 'e', so:

```
plain text     encryption rocks
key(repeated) alabastera labas
cipher text    eycsyhmmfn codkk
```