BACON

Sir Francis Bacon (1561-1626) invented a cipher in which the cipher equivalents are five-letter groups and the resulting cipher is monoalphabetic in character.

Bacon uses a 24 letter cipher with I and J, U and W used interchangeably.

A = aaaaa	I/J = abaaa	R = baaaa
B = aaaab	K = abaab	S = baaab
C = aaaba	L = ababa	T = baaba
D = aaabb	M = ababb	U/V = baabb
E = aabaa	N = abbaa	W = babaa
F = aabab	O = abbab	X = babab
G = aabba	P = abbba	Y = babba
H = aabbb	Q = abbbb	Z = babbb

Bacon described the steganographic effect of message enfolding in an innocent external message. Suppose we let capitals be the "a" element and lower-case letters represent the "b" elements. The message "All is well with me today" can be made to convey the message "Help." Thus:

```
A  L  l  i  s    W E l L   W    I t H  m E   T o d a Y
a  a  b  b  b    a a b a   a    a b a  b a   a b b b a

      H             E             L            P
```

Bacon describes many several variations on the theme. Note the regularity of construction of Bacon's biliteral alphabet, a feature which permits its reconstruction from memory.

[Excerpt from "Classical Cryptography Course" by Randy Nichols (LANAKI)]