# **Crypto Quiz**

Can you solve these ciphers for these towns and cities in Scotland:

|  |  |  |
| --- | --- | --- |
| Method | Cipher | Answer |
| **Substitution** | %65 %64 %69 %6E %62 %75 %72 %67 %68 |  |
| **Semaphore** |  |  |
| **Pigpen** |  |  |
| **Mary** |  |  |
| **Shifted** | NKXKPIUVQP |  |
| **Rot13** | Oryyfuvyy |  |
| **Morse** | (....) (.- --) (..) (.-..) (-) (---) (-.) |  |
| **Templar** |  |  |
| **Dscript** |  |  |
| **Braille** |  |  |
| **QR Code** |  |  |
| **Scrambled** | ADZPJMXCRA |  |
| **Polybius** | 13 34 11 44 12 42 24 14 22 15 |  |
| **Homophonic** | 11 07 04 24 19 25 31 10 |  |
| **Bacon** | AABBA BAAAA AABAA AABAA ABBAA ABBAB AAABA ABAAB |  |
| **ADFGVX** | DV VG VV AG VV XD |  |
| **Atbash** | RIERMV |  |
| **Navajo** | Be No-da-ih Na-as-tso-si Ma-e Gah Tkin Dzeh Dibeh |  |
| **Rail (3 rails)** | MERUSLUGSBH |  |
| **Porta**  **Key = “ab”** | PZLRRPNMX |  |
| **Pollux** | 08594 09074 24770 60860 183 |  |
| **Baudot** | [25-11001][1-00001][3-00011][10-01010][5-00101][9-01001][1-00001][12-01100] |  |
| **Dvorak** | APXPRAYD |  |
| **Vigenère**  **(Key=”king”)** | LQFNYXOXSOTY |  |

# Substitution

a (%61) b (%62) c (%63) d (%64) e (%65)

f (%66) g (%67) h (%68) i (%69) j (%6A)

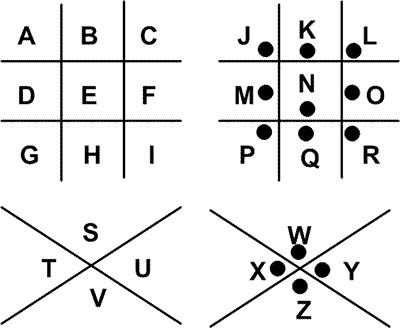
k (%6B) l (%6C) m (%6D) n (%6E) o (%6F)

p (%70) q (%71) r (%72) s (%73) t (%74)

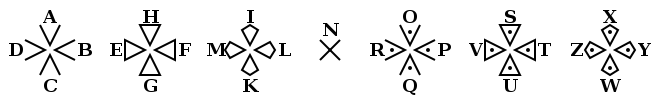
u (%75) v (%76) w (%77) x (%78) y (%79)

z (%80) SPACE (%20)

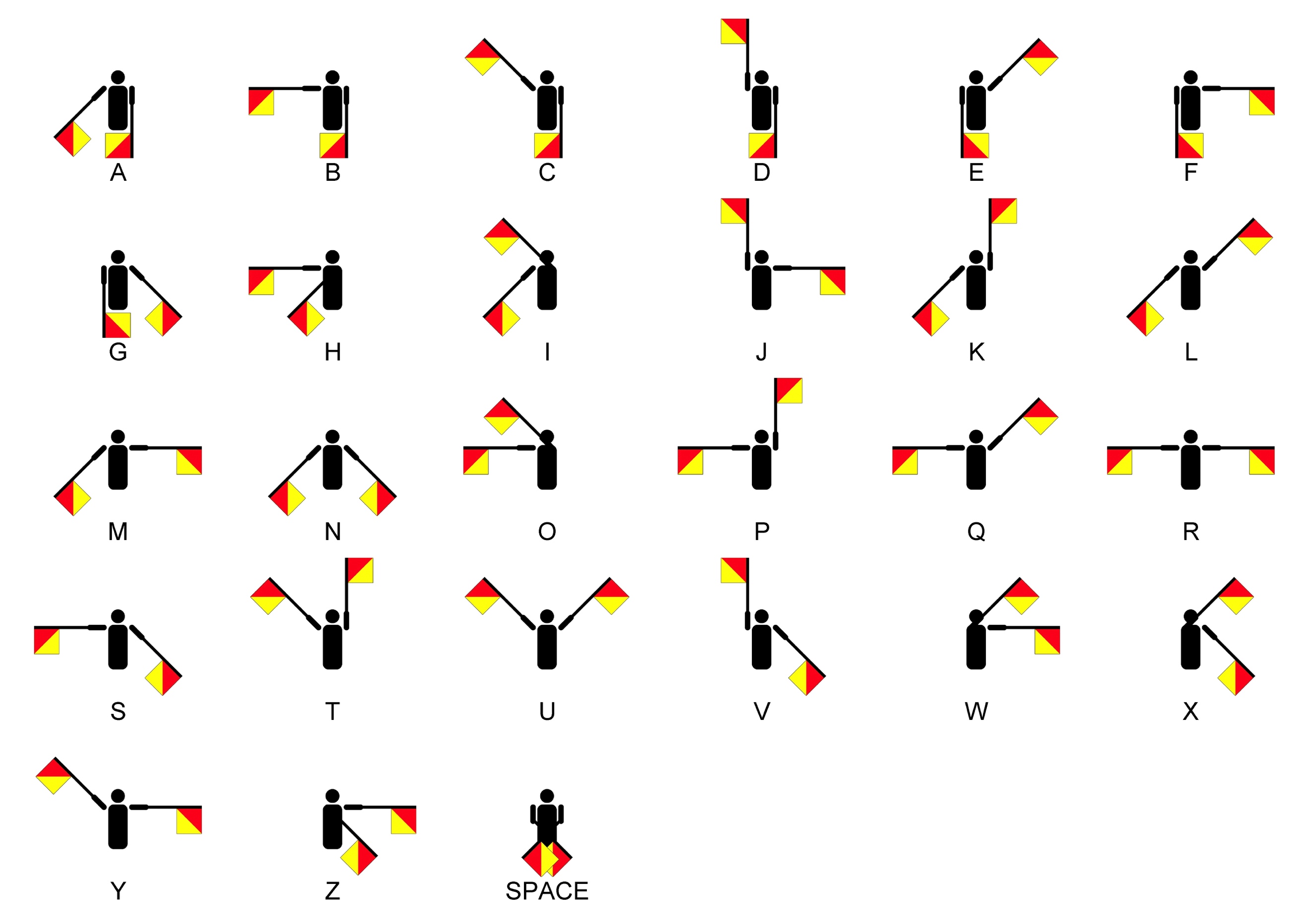
# Pigpen



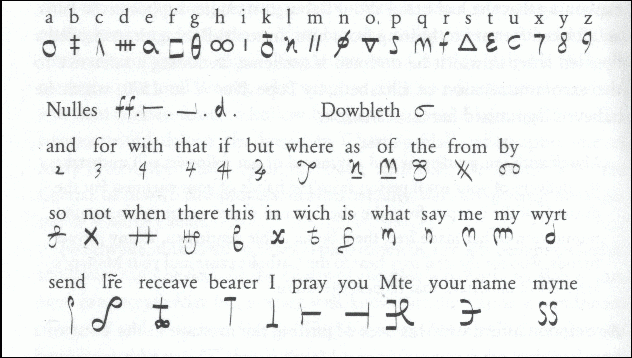
# Templar



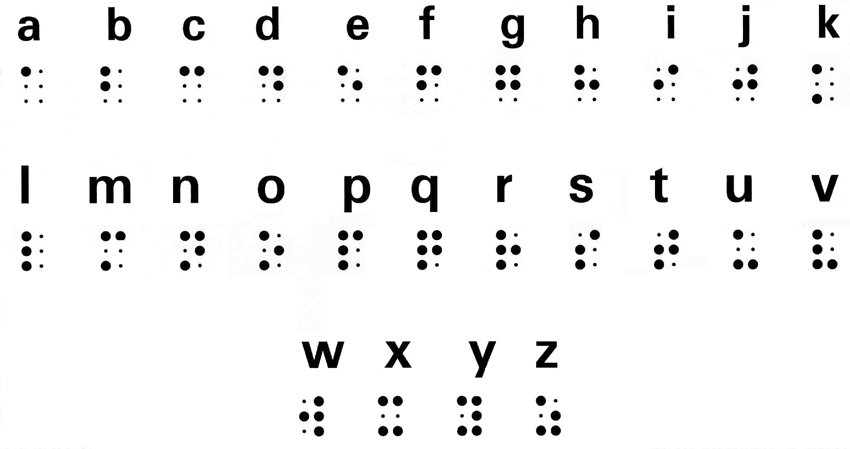
# Semaphore



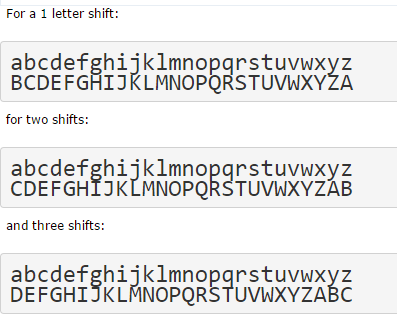
# Mary QoS



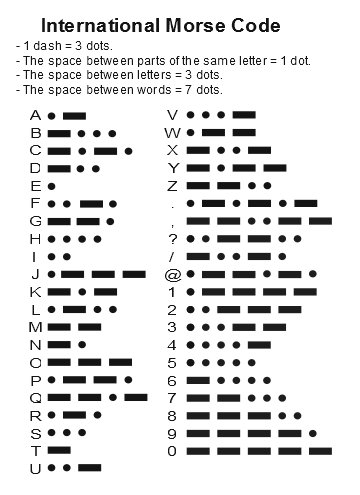
# Braille



# Shifted



# Morse



# Bacon

a AAAAA g AABBA n ABBAA t BAABA

b AAAAB h AABBB o ABBAB u-v BAABB

c AAABA i-j ABAAA p ABBBA w BABAA

d AAABB k ABAAB q ABBBB x BABAB

e AABAA l ABABA r BAAAA y BABBA

f AABAB m ABABB s BAAAB z BABBB

# Atbash

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: ZYXWVUTSRQPONMLKJIHGFEDCBA

# Bifid

1 2 3 4 5

1 B G W K Z

2 Q P N D S

3 I O A X E

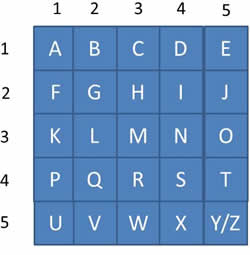
4 F C L U M

5 T H Y V R

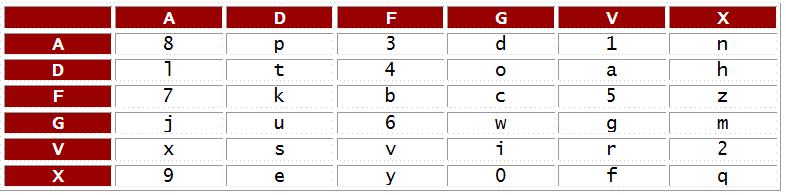
# Scrambled

|  |  |  |
| --- | --- | --- |
| Plaintext: | abcdefghijklmnopqrstuvwxyz |  |
| Scrambled code: | JTRNYLOHDBAZPXVEQMWICGKUFS |  |

# Polybius



# ADFGVX



# Navajo

|  |  |  |
| --- | --- | --- |
| **Alphabets (English)** | **Code Language (English)** | **Code Language (Navajo)** |
| A | Ant | Wol-la-chee |
| B | Bear | Shush |
| C | Cat | Moashi |
| D | Deer | Be |
| E | Elk | Dzeh |
| F | Fox | Ma-e |
| G | Goat | Klizzie |
| H | Horse | Lin |
| I | Ice | Tkin |
| J | Jackass | Tkele-cho-gi |
| K | Kid | Klizzie-yazzi |
| L | Lamb | Dibeh-yazzi |
| M | Mouse | Na-as-tso-si |
| N | Nut | Nesh-chee |
| O | Owl | Ne-ash-jsn |
| P | Pig | Bi-sodih |
| Q | Quiver | Ca-yeilth |
| R | Rabbit | Gah |
| S | Sheep | Dibeh |
| T | Turkey | Than-zie |
| U | Ute | No-da-ih |
| V | Victor | a-keh-di-glini |
| W | Weasel | Gloe-ih |
| X | Cross | Al-an-as-dzoh |
| Y | Yucca | Tsah-as-zih |
| Z | Zinc | Besh-do-gliz |

# Rail

'WE ARE DISCOVERED. FLEE AT ONCE', gives:

W . . . E . . . C . . . R . . . L . . . T . . . E

. E . R . D . S . O . E . E . F . E . A . O . C .

. . A . . . I . . . V . . . D . . . E . . . N . .

to give:

WECRL TEERD SOEEF EAOCA IVDEN

# Porta

Porta Cipher uses a polyalphabetic substitution cipher. It uses uses 13 alphabets, and which are reciprocal, thus enciphering becomes the same as deciphering.

Keys| 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

---------------------------------------------------------

A,B | n o p q r s t u v w x y z a b c d e f g h i j k l m

C,D | o p q r s t u v w x y z n m a b c d e f g h i j k l

E,F | p q r s t u v w x y z n o l m a b c d e f g h i j k

G,H | q r s t u v w x y z n o p k l m a b c d e f g h i j

I,J | r s t u v w x y z n o p q j k l m a b c d e f g h i

K,L | s t u v w x y z n o p q r i j k l m a b c d e f g h

M,N | t u v w x y z n o p q r s h i j k l m a b c d e f g

O,P | u v w x y z n o p q r s t g h i j k l m a b c d e f

Q,R | v w x y z n o p q r s t u f g h i j k l m a b c d e

S,T | w x y z n o p q r s t u v e f g h i j k l m a b c d

U,V | x y z n o p q r s t u v w d e f g h i j k l m a b c

W,X | y z n o p q r s t u v w x c d e f g h i j k l m a b

Y,Z | z n o p q r s t u v w x y b c d e f g h i j k l m a

# Pollux

This page defines the Pollux cipher [Theory](http://www.cs.ucf.edu/%7Egworley/files/pollux_and_frac_morse.txt). With this we use Morse code (see below) to determine a code, and then map a dot, dash or seperator with the following:

* Dot - 0, 7 or 4
* Dash - 1, 8 or 5
* Seperator - 2, 9, 6 or 3

For example "GE" becomes "— — ·" and "·", so we can then encode to 180 2 7 9 to give 180279.

# Baudot

Baudot coding was used with punched tape and has a 5-bit coding system.

0 1 2 3 4 5 6 7 8 9

'\*' 'E' '\n' 'A' ' ' 'S' 'I' 'U' '\r' 'D'

10 11 12 13 14 15 16 17 18 19

'R' 'J' 'N' 'F' 'C' 'K' 'T' 'Z' 'L' 'W'

20 21 22 23 24 25 26 27 28 29

'H' 'Y' 'P' 'Q' 'O' 'B' 'G' '' 'M' 'X',

# Dvorak

This type of coding maps the QWERTY keyboard to a Dvorak keyboard:

Plain: abcdefghijklmnopqrstuvwxyz

Cipher: axje.uidchtnmbrl'poygk,qf;

## Vigenère

With Vignere we move the cipher based on a keyword:

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

1  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 a

2  c d e f g h i j k l m n o p q r s t u v w x y z a b

3  d e f g h i j k l m n o p q r s t u v w x y z a b c

4  e f g h i j k l m n o p q r s t u v w x y z a b c d

5  f g h i j k l m n o p q r s t u v w x y z a b c d e

6  g h i j k l m n o p q r s t u v w x y z a b c d e f

7  h i j k l m n o p q r s t u v w x y z a b c d e f g

8  i j k l m n o p q r s t u v w x y z a b c d e f g h

9  j k l m n o p q r s t u v w x y z a b c d e f g h i

10  k l m n o p q r s t u v w x y z a b c d e f g h i j

11  l m n o p q r s t u v w x y z a b c d e f g h i j k

12  m n o p q r s t u v w x y z a b c d e f g h i j k l

13  n o p q r s t u v w x y z a b c d e f g h i j k l m

14  o p q r s t u v w x y z a b c d e f g h i j k l m n

15  p q r s t u v w x y z a b c d e f g h i j k l m n o

16  q r s t u v w x y z a b c d e f g h i j k l m n o p

17  r s t u v w x y z a b c d e f g h i j k l m n o p q

18  s t u v w x y z a b c d e f g h i j k l m n o p q r

19  t u v w x y z a b c d e f g h i j k l m n o p q r s

20  u v w x y z a b c d e f g h i j k l m n o p q r s t

21  v w x y z a b c d e f g h i j k l m n o p q r s t u

22  w x y z a b c d e f g h i j k l m n o p q r s t u v

23  x y z a b c d e f g h i j k l m n o p q r s t u v w

24  y z a b c d e f g h i j k l m n o p q r s t u v w x

25  z 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

For example, if we use a key of KING:

**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**

6  g h i j k l m n o p q r s t u v w x y z a b c d e f

8  i j k l m n o p q r s t u v w x y z a b c d e f g h

10  k l m n o p q r s t u v w x y z a b c d e f g h i j

13  n o p q r s t u v w x y z a b c d e f g h i j k l m

For example **phase** becomes **zpnyo**, as **p** (read row 10 for **K**) gives **Z**, h (read row 8 for I) gives P, a (read row 13 for N) gives n), and so on.

The great advantage of this type of code is that the same plaintext character will be encrypted with different values, depending on the position of the keyword. For example, if the keyword is GREEN, ‘e’ can be encrypted as ‘K’ (for G), ‘V’ (for R), ‘I’ (for E) and ‘R’ (for N).

# Rot13

Rot13 Cipher, which is a Caeser cipher with a shift of 13 spaces::

abcdefghijklmnopqrstuvwxyz

NOPQRSTUVWXYZABCDEFGHIJKLM

# Dscript



# Homophonic

We allocate codes in relation to the frequency of the letters in normal English:

