

## On the Subject of The Hill Cycle

*Not the kind you need a mountain bike for.*

This module consists of a screen, eight dials with blue labels, and a QWERTY keyboard.

The labels on the dials, when decrypted and read from left to right, spell out an eight letter word.

The eight dials can be split into four pairs of adjacent dials, each with one upper and one lower dial.

The number of  $72^\circ$  rotations, starting from north, of each pair is interpreted as two digit base 5 numbers.

These numbers give the entries of a  $2 \times 2$  matrix in reading order.

The alphabetic positions of the letters on these pairs of dials modulo 26 become entries in  $2 \times 1$  column vectors.

Each vector is multiplied by the matrix and taken modulo 26 to produce the a vector whose entries are the alphabetic positions of the encrypted letters.  
(with Z=0)

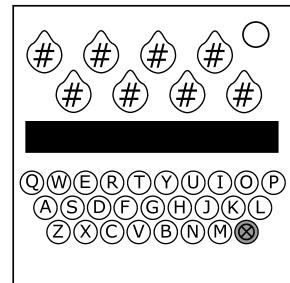
Once deciphered, find the word in the table below, the word written below it is the word that should be entered.

Apply the same encryption to the response word, and type out the encrypted response word using the keys.

The word is automatically submitted when eight keys are pressed.

The red button can be pressed at any time before the eighth key is pressed to cancel the input.

Inputting any of the eight letters incorrectly will cause a strike to be issued and reset the module.



### Decrypting a Hill cipher

The encryption process utilises matrix multiplication:

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} X' \\ Y' \end{bmatrix}$$

To undo this process, the inverse matrix must be found:

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}^{-1} \begin{bmatrix} X' \\ Y' \end{bmatrix} = \begin{bmatrix} X \\ Y \end{bmatrix}$$

First, find the adjugate of the key matrix:

$$\text{adj} \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \begin{bmatrix} D & -B \\ -C & A \end{bmatrix}$$

Then, find the multiplicative inverse of the determinant of the matrix, N:

$$\det \begin{bmatrix} A & B \\ C & D \end{bmatrix} = AD - BC$$

$$N(AD - BC) \bmod 26 = 1$$

(Multiplicative inverses must also be found to decrypt affine enciphered messages.)

The inverse matrix is the adjugate matrix multiplied by the multiplicative inverse:

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix}^{-1} = N \begin{bmatrix} D & -B \\ -C & A \end{bmatrix}$$

The alphabetic positions of each encrypted pair of letters can be multiplied by the inverse matrix to retrieve the original message.

## Keyword Table