

## On the Subject of The Ultimate Cycle

*How much security does one word need?*

This module consists of a screen, eight dials with red 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 word has been encrypted through a series of ciphers, indicated by the direction each dial is pointing, from left to right.

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

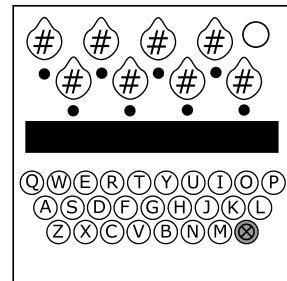
Apply the same sequence of encryptions to the response word, and type out the encrypted response word using the keys.

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.

**Note:** Unless stated otherwise, any reference to a letter's alphabetic position starts at A = 1. Similarly, any reference to the position of a dial starts from the leftmost dial = 1.



## N: Atbash Logic Cipher

### Logic component

For each dial: if the number of  $45^\circ$  rotations, starting from north, is odd, then the bit given by the dial is 1. Otherwise, it is 0.

Form four pairs of bits by grouping the bits corresponding to adjacent pairs of dials from left to right.

Form another four pairs of bits by grouping the bits corresponding to adjacent pairs of dials in reading order.

Each of the eight pairs of bits correspond to each of the eight dials from left to right.

Using the operator corresponding to the position of the north pointing dial, find the truth values of each pair; the encrypted letter depends on whether each is true or false.

|  | AND | OR | XOR | $\Rightarrow$ | NAND | NOR | XNOR | $\Leftarrow$ |
|--|-----|----|-----|---------------|------|-----|------|--------------|
|--|-----|----|-----|---------------|------|-----|------|--------------|

|       | Letter | 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 |
|-------|--------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| True  | U      | F | Z | W | D | B | V | C | L | S | H | I | J | M | N | Q | G | X | K | Y | T | E | O | P | R | A |   |
| False | N      | V | Y | P | W | A | H | O | Q | C | M | U | G | F | D | I | R | L | T | X | B | S | K | Z | J | E |   |

### Atbash component

Each letter in the word is swapped with the letter with the same alphabetic position in the reversed alphabet.

That is, a letter with alphabetic position X will become the letter with alphabetic position  $27 - X$ .

If the LED below the north pointing dial is lit, the Atbash cipher is applied to the input of the Logic cipher.

Otherwise, the Atbash cipher is applied to the output of the Logic cipher.

## NE: Caesar Cipher

Each letter in the word has been shifted forwards through the alphabet by the position of the dial corresponding to this cipher.

If the LED corresponding to this dial is lit, each letter is then shifted further by the number of  $45^\circ$  rotations, starting from north, to the direction each dial is pointing.

Otherwise, each letter is then shifted backwards through the alphabet by the number of  $45^\circ$  rotations, starting from north, to the direction each dial is pointing.

## E: Playfair Cipher

The indexing of the lists start at zero.

- If the last dial is pointing south, use the word corresponding to the number of 45° rotations, starting from north, of the first dial.
- Otherwise, the number of rotations, starting from north, of the next dial corresponds to which of the words in the lists below is the keyword for this cipher.
  - If there are less than three unique\* ports on the bomb, use the keyword from List A.
  - Otherwise, use the keyword from List B.
- The keyword gives the first ten letters of the keysquare.
  - If the LED corresponding to this cipher is unlit, the keyword is entered into the keysquare in reading order.
  - Otherwise, the keyword is entered into the keysquare in reverse reading order.
- The remaining 15 letters fill the rest of the keysquare in alphabetical order, excluding X, which is never used.
- The word is split into four pairs of letters.
- Each pair of letters is altered:
  - If both letters are the same, the encrypted pair is two of the letter diametrically opposite in the keysquare.
  - Otherwise, if both letters belong to the same row of the keysquare, shift both letters one space to the right along the row.
  - Otherwise, if both letters belong to the same column of the keysquare, shift both letters once space down the column.
  - Otherwise, the letters lie on diagonally opposite corners of a rectangle, the encrypted pair consists of the letters in the horizontally opposite corners from the original pair.

\*A port is unique if there is only one of its type on the bomb.

List A: ALGORITHMS, AUTHORIZED, BLUEPRINTS, DESPICABLY, FORMIDABLE, HYPERBOLIC, IMPORTANCE, LABYRINTHS

List B: WANDERLUST, VANQUISHED, ULTRASONIC, SCRAMBLING, PRECAUTION, OSTRACIZED, METHODICAL, MAGNITUDES

### Important:

- If the pair of letters is XX, the pair is unchanged by the cipher.
  - If the pair of letters is either X# or #X, where # is not X, the X is changed to the other letter, forming a double letter pair, and enciphered normally.
- Then, the new letter is changed back to an X.

## SE: Pigpen Cipher

Each letter is translated using one of the two pigpen ciphers below.

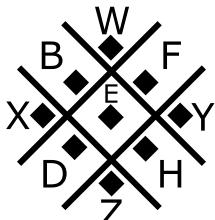
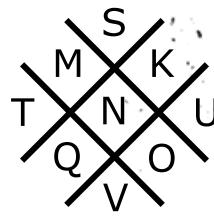
Starting from north, the pigpen characters are rotated to face the direction the dial is pointing. The rotated pigpen characters are then translated back, as though they are still facing north, to produce the encrypted letter.

If the LED corresponding to this cipher is unlit, use cipher I. Otherwise, use cipher II.

### Cipher I

|   |   |   |
|---|---|---|
| A | B | C |
| D | E | F |
| G | H | I |

|   |   |   |
|---|---|---|
| J | K | L |
| M | N | O |
| P | Q | R |



### Cipher II

|   |   |   |
|---|---|---|
| A | C | E |
| G | I | K |
| M | O | Q |

|   |   |   |
|---|---|---|
| S |   |   |
| U | H | D |
| P | J | L |
| Y |   |   |

|   |   |   |
|---|---|---|
| B | D | F |
| H | J | L |
| N | P | R |



## S: Two Square Cipher

The indexing of the lists start at 0. For this cipher, the leftmost dial has a position of 0.

- The two lists give the keywords for two 5x5 keysquares, the keyword from List A is used for the first keysquare and the keyword from List B is used for the second:
  - If the numbers in the serial number add up to more than 9, the keyword in List A is given by the position of dial and the keyword in List B is given by the number of 45° rotations, starting from north, of the **previous** dial.
  - Otherwise, the keyword in List B is given by the position of dial and the keyword in List A is given by the number of 45° rotations, starting from north, of the **previous** dial.
  - If the first dial is pointing south, the 'previous' dial is the last dial.
- These keywords fill the first two rows of their respective keysquares in reading order. The remaining 15 letters of each keysquare fill them in alphabetical order, excluding X, which is never used.
- The word is split into four pairs of letters. For each pair, the first letter is found in the first keysquare and the second is found in the second keysquare.
- If the LED below the south pointing dial is lit:
  - The keysquares are arranged horizontally, with the first keysquare to the left of the second.
  - The letters lie on diagonally opposite corners of a rectangle between the two keysquares. The encrypted pair consists of the letters in the corners horizontally opposite from the original pair.
- If the LED below the south pointing dial is unlit:
  - The keysquares are arranged vertically, with the first keysquare above the second.
  - The letters lie on diagonally opposite corners of a rectangle between the two keysquares. The encrypted pair consists of the letters in the corner vertically opposite from the original pair.

List A: AFTERSHOCK, DESTROYING, DUPLICATES, FAR-SIGHTED, GRACIOUSLY, INFAMOUSLY, NIGHTMARES, PALINDROME

List B: DOWNSTREAM, EMORDNIALP, FLASHPOINT, INTRODUCES, PATHFINDER, QUADRIGEPS, TRAPEZOIDS, WAVERINGLY

### **Important:**

- If the pair of letters is XX, the pair is unchanged by the cipher.
- If the pair of letters is either X# or #X, where # is not X, the X is changed to the other letter, forming a double letter pair, and enciphered normally.  
Then, the new letter is changed back to an X.

## SW: Monoalphabetic Substitution Cipher

The position of the dial corresponds to which of the eight words in the list below is the keyword for this cipher:

DOCUMENTARILY, FLAMETHROWING, FLOWCHARTINGS, HYDROMAGNETIC, METALWORKINGS, MULTIBRANCHED, TROUBLEMAKING, UNPREDICTABLY

If the LED is unlit, the remaining thirteen letters of the alphabet are left in alphabetical order. Otherwise, the remaining thirteen letters are positioned in reverse alphabetical order.

- If there are an even number of batteries, the keyword precedes the remaining letters to construct a cipher alphabet.
- Otherwise, the keyword follows the remaining letters to construct a cipher alphabet.

Each letter of the alphabet is mapped onto the letter of the cipher alphabet with the same alphabetic position.

The letters in the word change accordingly with these mappings.

### W: Hill Cipher

If there are more lit than unlit indicators, the keyword for this cipher belongs to list A. Otherwise the keyword for this cipher belongs to list B.

The keyword used depends and the rotations of the dials adjacent to the one corresponding to this cipher:

The indexing of the lists start at zero.

- If the first dial is pointing west, use the keyword corresponding to six plus the number of 45° rotations, starting from north, of the second dial.
- If the last dial is pointing west, use the keyword corresponding to six plus the number of 45° rotations, starting from north, of the seventh dial.
- Otherwise, use the keyword corresponding to the sum of the numbers of 45° rotations, starting from north, of the two dials adjacent to this one.

**List A:** AEON, COPY, EACH, GOOD, IOTA, KILO, MARK, ONCE, QUIT, RIOT, SYNC, UNDO, WORK, YEAR, ZEAL

**List B:** BOMB, BUSY, DICE, FAUX, HUSK, JUKE, LIMA, LOCI, NAME, PUSH, RISE, TASK, VOID, XYST, ZOOM

The alphabetic positions of the letters in the keyword modulo 26 form the entries of a 2x2 square keymatrix in reading order.

If the LED corresponding to this cipher is lit, the matrix is then transposed, swapping its top-right and bottom-left entries.

The word to be enciphered is broken into four pairs of letters and their alphabetic positions modulo 26 form entries in 2x1 vectors.

The vectors are multiplied by the keymatrix and taken modulo 26 to obtain the alphabetic positions of the encrypted pairs of letters.

(Because Z has an alphabetic position of 26, its corresponding entry in the encrypted vector is zero.)

### NW: Bitshift Cipher

Find the 3 digit binary representations the numbers of rotations, starting from north, of each of the dials.

If the LED corresponding to a dial is lit, swap the 0s for 1s and the 1s for 0s in its binary representation.

Combine all of the binary representations together, from left to right.

Prepend a 0 and append a 1 to the combined binary representations to produce a 26 bit string.

Separate the alphabet into two sets, depending on whether each letter's alphabetic position in the string of bits is a 1 or a 0.

The letters in these sets remain in alphabetical order.

If the LED corresponding to the NW dial is lit, each letter in the word is shifted to the right by the position of the NW dial.

Otherwise, each letter is shifted to the left by the position of the NW dial.

Keyword Table

|          |          |          |          |          |          |          |          |
|----------|----------|----------|----------|----------|----------|----------|----------|
| ADVANCED | ADVERTED | ADVOCATE | ADDITION | ALLOCATE | ALLOTYPE | ALLOTTED | ALTERING |
| PROGRESS | ZYGOTENE | QUARTICS | LINKAGES | QUICKEST | ORDERING | UNDOINGS | ZUGZWANG |
| BINARIES | BINORMAL | BINOMIAL | BILLIONS | BULKHEAD | BULLHORN | BULLETED | BULWARKS |
| YOKOZUNA | COMMANDO | GLOOMING | TRICKIER | GATEWAYS | INCOMING | ZYGMATA  | FORMULAE |
| CIPHERED | CIRCUITS | CONNECTS | CONQUERS | COMMANDO | COMPILER | COMPUTER | CONTINUE |
| BULKHEAD | RELATION | LINKWORK | NANOTUBE | MONOTONE | YIELDING | ILLUMINE | KILOBYTE |
| DECRYPTS | DECEIVED | DECIMATE | DIVISION | DISCOVER | DISCRETE | DISPATCH | DISPOSAL |
| NANOBOTS | QUINTICS | ZIGZAGGY | MONOMIAL | ULTERIOR | KNUCKLED | UNDERWAY | ULTRARED |
| ENCIPHER | ENCRYPTS | ENCODING | ENTRANCE | EQUALISE | EQUATORS | EQUATION | EQUIPPED |
| JUNKYARD | QUADRANT | TRIANGLE | RELAYING | NANOGRAM | CONNECTS | INDICATE | BINORMAL |
| FINALISE | FINISHED | FINDINGS | FINNICKY | FORMULAE | FORTUNES | FORTRESS | FORWARDS |
| DISCRETE | JUNCTION | KILOWATT | ROTATION | POSITRON | DISPATCH | ENCIPHER | STANDOUT |
| GARRISON | GARNERED | GATEPOST | GATEWAYS | GAUNTLET | GAMBLING | GATHERED | GLOOMING |
| STOCKADE | FINDINGS | ADVANCED | JOURNEYS | STOPPING | LANDMARK | EQUATION | VICELESS |
| HAZARDED | HAZINESS | HOTLINKS | HOTHEADS | HUNDREDS | HUNKERED | HUNTSMAN | HUNTRESS |
| DISCOVER | JUNCTURE | TOGETHER | GARRISON | WHATNOTS | DIVISION | TOGGLING | YEASAYER |
| INCOMING | INDICATE | INDIRECT | INDIGOES | ILLUDING | ILLUSION | ILLUSORY | ILLUMINE |
| VENOMOUS | FORTUNES | OBSERVED | QUITTERS | HUNKERED | HOTHEADS | TOMOGRAM | KNOWABLE |
| JIGSAWED | JIMMYING | JOURNEYS | JOUSTING | JUNCTURE | JUNCTION | JUNKYARD | JUDGMENT |
| YEARNING | TRIGONAL | VOLITION | DECRYPTS | LABELING | STARTING | OCTUPLES | ROTATORS |
| KILOWATT | KILOVOLT | KILOBYTE | KINETICS | KNOCKING | KNOCKOUT | KNOWABLE | KNUCKLED |
| POSITIVE | BILLIONS | WHATEVER | FINALISE | ENCRYPTS | OBSTACLE | ENCODING | ADVOCATE |
| LANGUAGE | LANDMARK | LIMITING | LINEARLY | LINGERED | LINKAGES | LINKWORK | LABELING |
| CONQUERS | EQUATION | GATEPOST | ILLUSION | QUIRKISH | NUMERATE | STANDARD | POSTSYNC |
| MONOGRAM | MONOLITH | MONOMIAL | MONOTONE | MULTITON | MULTIPLY | MULCTING | MULLIGAN |
| HUNTRESS | WINNABLE | ZYMOLOGY | ILLUSORY | VOLATILE | TOMAHAWK | OCTANGLE | ADVERTED |

Keyword Table cont.

|          |          |          |          |          |          |          |          |
|----------|----------|----------|----------|----------|----------|----------|----------|
| NANOBOTS | NANOGRAM | NANOWATT | NANOTUBE | NUMBERED | NUMEROUS | NUMERALS | NUMERATE |
| ZIPPERED | STOCCATA | VENDETTA | LINGERED | FINNICKY | JUDGMENT | HUNDREDS | ILLUDING |
| OCTUPLES | OCTANGLE | ORDERING | ORDINALS | OBSERVED | OBSCURED | OBSTRUCT | OBSTACLE |
| KNOCKING | WINGDING | UNDERLIE | LINEARLY | TRIGGERS | PROJECTS | ALLOTYPE | YIELDERS |
| PROGRESS | PROJECTS | PROPHASE | PROPHECY | POSTSYNC | POSSIBLE | POSITRON | POSITIVE |
| JIGSAWED | KILOVOLT | ALLOTTED | RELATIVE | PROPHASE | COMPILER | LIMITING | NANOWATT |
| QUADRANT | QUADRICS | QUARTILE | QUARTICS | QUICKEST | QUIRKISH | QUINTICS | QUITTERS |
| YELLOWED | MULCTING | GATHERED | WEAKENED | WHATNESS | HAZINESS | REVOLVED | ENTRANCE |
| REVERSED | REVOLVED | REVEALED | ROTATION | ROTATORS | RELATION | RELATIVE | RELAYING |
| FORTRESS | WHATSITS | BULLHORN | GARNERED | INDIGOES | LANGUAGE | CIRCUITS | VOLTAGES |
| STARTING | STANDARD | STANDOUT | STANZAIC | STOCCATA | STOCKADE | STOPPING | STOPWORD |
| REVERSED | JIMMYING | DECEIVED | QUARTILE | GAUNTLET | HAZARDED | MULTIPLY | ZYMOGRAM |
| TRICKIER | TRIGONAL | TRIGGERS | TRIANGLE | TOMOGRAM | TOMAHAWK | TOGLLING | TOGETHER |
| MULLIGAN | ZIGGURAT | ALLOCATE | NUMERALS | BULWARKS | BINARIES | INDIRECT | REVEALED |
| UNDERRUN | UNDERWAY | UNDERLIE | UNDOINGS | ULTERIOR | ULTIMATE | ULTRARED | ULTRAHOT |
| JOUSTING | VICINITY | QUADRICS | MONOLITH | ORDINALS | KNOCKOUT | NUMEROUS | STOPWORD |
| VENOMOUS | VENDETTA | VICINITY | VICELESS | VOLITION | VOLTAGES | VOLATILE | VOLUMING |
| UNDERRUN | DISPOSAL | WEAPONED | HUNTSMAN | BULLETED | ALTERING | MONOGRAM | POSSIBLE |
| WEAKENED | WEAPONED | WINGDING | WINNABLE | WHATEVER | WHATNESS | WHATNOTS | WHATSITS |
| EQUALISE | OBSTRUCT | COMPUTER | STANZAIC | DECIMATE | EQUIPPED | BINOMIAL | YEARLONG |
| YELLOWED | YEARLONG | YEARNING | YEASAYER | YIELDING | YIELDERS | YOKOZUNA | YOURSELF |
| CIPHERED | CONTINUE | KINETICS | FORWARDS | ADDITION | FINISHED | GAMBLING | MULTITON |
| ZIPPERED | ZIGGURAT | ZIGZAGGY | ZUGZWANG | ZYgomata | Zygogene | Zymology | Zyogram  |
| VOLUMING | ULTIMATE | HOTLINKS | NUMBERED | PROPHECY | YOURSELF | ULTRAHOT | OBSCURED |