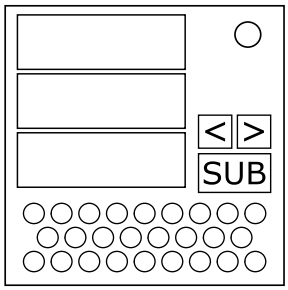
On the Subject of The Cornflower Cipher



Centaureae cyani colores pulchros habent.

On the module, you will see 3 screens, a keyboard, 2 arrows, and a submit button that displays the current page you're on.

Pressing the right arrow takes you to the next page. Pressing the left arrow takes you to the previous page. There is a total of 2 pages.

To prepare, interpret the first character of the serial number as a base-36 digit and convert it to a 6-digit binary number. This manual will refer to the individual digits of this binary number as "bit 1", "bit 2", "bit 4", "bit 8", and "bit 16". (Bit 32 is ignored.)

Step 1: Ping-pong Straddling Checkerboard Cipher

For this step, concatenate the last screen on page 1 and the first screen on page 2. This will be referred to as the coded word. You will also need the words on the middle and bottom screens on page 2, called KW1 and KW2, respectively.

In this step, we will create two straddling checkerboards. We will use the first one to convert the coded word into a bunch of digits, and the second to convert those digits back into letters.

For the first straddling checkerboard, obtain the following numbers:

- d1 = number of indicators, modulo 6
- d2 = number of ports, modulo 6; if equal to d1, add 1 and modulo 6 again

Also create an alphabet key from KW1 as follows:

- Remove all duplicate letters from the keyword (retain first occurrences).
- Write the entire alphabet with the letters from the keyword removed.
- If bit 8 is 1, place the alphabet after the keyword, otherwise before.

To create a straddling checkerboard, start with a table with 5 rows and 6 columns. Label the columns with the numbers 0–5. Cross out all the first-row cells except for those in columns labeled d1 and d2. Fill the remaining 26 cells with the alphabet key. If bit 16 is 1, use column order (fill the first column from top to bottom, then the second column etc.); otherwise, use reading order.

Also label the rows except the first with the numbers 0–5 but omitting d1 and d2.

Now convert every letter from the coded word to digits. Each letter that occurs in the first row gets turned into the single digit that labels its column; all other letters turn into digits labeling the row followed by the column.

Now create the second straddling checkerboard as before, but with the following changes:

- Instead of d1 & d2, use the following numbers:
  - d3 = number of batteries, modulo 6
  - d4 = number of lit indicators, modulo 6; if equal to d3, add 1 and modulo 6 again
- Instead of KW1 and bit 8, use KW2 and bit 2 to create the alphabet key.
- Instead of bit 16, decide the fill order using bit 4.

Convert the string of digits back into letters. If the first digit is d3 or d4, use the corresponding letter from the first row. Otherwise, use a pair of digits, where the first identifies the row and the second the column, to obtain a letter. If you are left with a single row digit, ignore it.

Once completed, this process produces a new keyword, KW3.

Example

Encrypted Word: GOEHXUWBL
KW1: EXTRAS, d1 = 2, d2 = 3; KW2: TRADING, d3 = 2, d4 = 0
Bits: 01100

EXTRAS + alphabet; reading order

	0	1	2	3	4	5
	#	#	E	X	#	#
0	T	R	A	S	B	C
1	D	F	G	H	I	J
4	K	L	M	N	O	P
5	Q	U	V	W	Y	Z

G → 12, O → 44, E → 2, H → 13, X → 3,
U → 51, W → 53, B → 04, L → 41
Digits: 1244213351530441

alphabet + TRADING; column order

	0	1	2	3	4	5
	B	#	O	#	#	#
1	C	J	P	V	Z	D
3	E	K	Q	W	T	I
4	F	L	S	X	R	N
5	H	M	U	Y	A	G

12 → P, 44 → R, 2 → O, 13 → V, 35 → I,
15 → D, 30 → E, 44 → R, 1 (discard)
KW3: PROVIDER

Step 2: Stunted Blind Polybius Cipher

This step requires the 8-letter keyword KW3 obtained from step 1 and the encrypted word concatenated from the top and middle screen on page 1.

The following diagrams will be used:

	1	2	3	4
1				
2				
3				
4				

	?	?	?	?
?	○○ ○○	●○ ○○	○● ○○	●● ○○
?	○○ ●○	●○ ●○	○● ●○	●● ●○
?	○○ ○●	●○ ○●	○● ○●	●● ○●
?	○○ ●●	●○ ●●	○● ●●	●● ●●

Begin by filling the Stunted Polybius square (left) with the letters A-P. Start with KW3. Remove all duplicated letters (retain first occurrences) and remove all letters Q-Z. Write the remaining letters A-P in alphabetical order with the letters from KW3 removed. If bit 1 is 1, place the alphabet after the keyword, otherwise before. Write these 16 letters into the grid in reading order.

Now label the rows and column of the Blind Polybius Square (right). The columns are labeled with numbers 1-4 in an order based on the first 4 letters of KW3. Label these letters 1-4 in alphabetical order. In case of recurring letters, label those from left to right. Proceed similarly to label the rows with numbers 1-4 in an order based on the last 4 letters of KW3.

Now convert the encrypted word, letter by letter, into dot patterns. Find each letter in the Stunted Polybius Square and determine its row and column, then find the dot pattern in the Blind Polybius Square using the matching row and column numbers.

Finally, stack the dot patterns on top of one another, then re-divide them into blocks of three rows each, and read the result as [Unified English Braille (https://ktane.timwi.de/HTML/Braille.html)](https://ktane.timwi.de/HTML/Braille.html) to obtain the encrypted word for the next step.

Example

Encrypted word: OCMOAOPCA
KW3: PROVIDER; bits: 01100

PROV → 2314
IDER → 3124

	1	2	3	4
1	A	B	C	F
2	G	H	J	K
3	L	M	N	P
4	O	I	D	E

	2	3	1	4
3	○○ ○○	●○ ○○	○● ○○	●● ○○
1	○○ ●○	●○ ●○	○● ●○	●● ●○
2	○○ ○●	●○ ○●	○● ○●	●● ○●
4	○○ ●●	●○ ●●	○● ●●	●● ●●

O → r4c1 → ○●/●●
C → r1c3 → ●○/●○
M → r3c2 → ○○/○○
O → r4c1 → ○●/●●
A → r1c1 → ○●/●○
O → r4c1 → ○●/●●
P → r3c4 → ●●/○○
C → r1c3 → ●○/●○
A → r1c1 → ○●/●○

Braille = TAWZMO

Step 3: Chain Rotation Cipher

Use the encrypted word from Step 2. The first letter remains the same. The second letter must be Caesar-shifted forward by the alphabetic position of the first letter. Each subsequent letter must be shifted forward by the alphabetic position of the previously obtained letter. Once completed, the result is your decrypted word.

Example

Encrypted word: TAWZMO
T, T+A = U, U+W = R, R+Z = R, R+M = E, E+O = T
Result: TURRET

Once you finally have your decrypted word, you can submit it. Once you start typing, all the screens will go black and the bottom screen will show what you are typing.

To clear it, just click one of the arrows. This goes to one of the pages and clears any input you put in. It will not let you go over 6 letters on input.

Once you are satisfied with your input, press the button labeled "SUB" to submit your answer. On a strike, the module will go back to the first page of the module, but it does not regenerate.