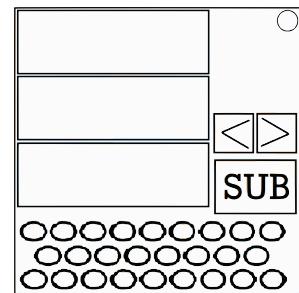


## On the Subject of the Ultimate Cipher

All ciphering techniques are required to solve this module.

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 5 pages.



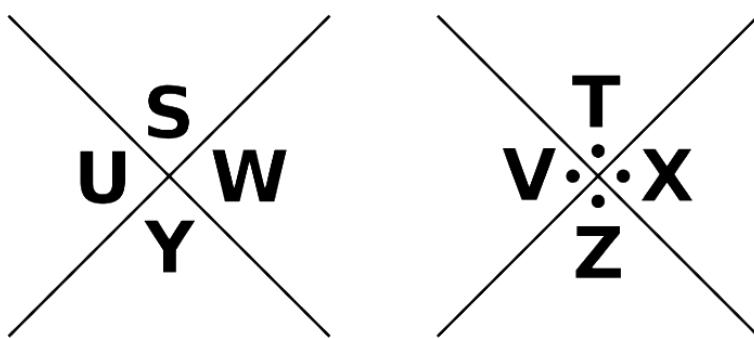
- Page 1: Top screen shows 6 symbols, the 2 screens below show 6 digit numbers.
- Page 2: Top screen shows a word. Middle screen shows a 6 digit binary number. Bottom screen shows a number.
- Page 3: Top screen shows a letter followed by roman numerals. Middle screen shows 3 letters. Bottom screen shows a number of paired letters.
- Page 4: All 3 screens show a word.
- Page 5: Top screen shows 6 symbols.

To disarm this module, you have to decrypt the word using the mechanics down below.

### Step 1: Pigpen Cipher

On page 1, the top screen shows 6 symbols. Decrypt it by using the pigpen cipher below

A	C	E	B	D	F
G	I	K	H	J	L
M	O	Q	N	P	R



### Step 2: Letter Transposition

For this, you will need the 2 numbers on the screens below the top screen. Take the 1st number from the middle screen to use for the column. Then take the 1st number from the bottom screen to use for the row. Use both numbers of the table below to get an instruction.

	0	1	2	3	4	5	6	7	8	9
0	34	16	14	24	25	23	45	34	R4	24
1	26	14	RV	15	R2	34	56	R3	26	25
2	23	RV	R1	RV	12	25	36	46	R2	25
3	35	12	46	24	45	R5	13	15	26	R5
4	R1	13	14	16	35	12	35	R3	25	R4
5	23	45	R3	46	16	36	R4	R5	34	R2
6	13	12	RV	12	R3	35	36	15	36	23
7	45	24	56	R4	R5	R2	35	23	56	46
8	RV	26	R1	13	13	56	15	15	24	34
9	36	R1	14	56	16	45	16	14	26	46

- ##: Switch the 2 letters at those positions.
- R#: Shift the whole word to the right # times.
- RV: Reverse the entire sequence.

Do this for each digit on the 2 screens to complete the transposition process.

### Step 3: Vigenere Cipher

On page 2 of the module, the top screen shows a word

Take the first letter of your encrypted word and the first letter on the top screen and translate them into numbers using the table below.

Add the two numbers together, and then turn them back into a letter with the same table.

If the numbers add up to something above 25, subtract 26 until the number is between 0 – 25.

Repeat for each letter.

A	8	H	13	0	14	V	9
B	0	I	7	P	3	W	17

C	16	J	22	Q	19	X	15
D	12	K	23	R	4	Y	20
E	5	L	6	S	21	Z	24
F	11	M	18	T	25		
G	10	N	1	U	2		

#### Step 4: Atbash Bit Switch

On page 2 of the module, the middle screen shows a 6 digit binary number that will be used later.

For now, first determine the scrambler that will be used by using the first character of the serial number:

0	21453	9	23154	I	24513	R	24531
1	21534	A	25134	J	25413	S	25431
2	31524	B	24153	K	34512	T	34521
3	31452	C	34152	L	35214	U	35421
4	41523	D	35124	M	35412	V	43251
5	41532	E	45123	N	43512	W	43521
6	51234	F	45132	O	45213	X	45231
7	51423	G	54123	P	53412	Y	53421
8	51432	H	54132	Q	54213	Z	54231

Next turn each letter of the encrypted word you have so far into it's alphanumeric position (A = 1, B = 2...Z = 26). Then turn each number into it's binary sequence using the table below:

1	00001	8	01000	15	01111	22	10110
2	00010	9	01001	16	10000	23	10111
3	00011	10	01010	17	10001	24	11000
4	00100	11	01011	18	10010	25	11001
5	00101	12	01100	19	10011	26	11010
6	00110	13	01101	20	10100		
7	00111	14	01110	21	10101		

For each binary sequence, run it through the scrambler so that the number in each position turns into that position of that number in the binary. Ex: 35124: 10011 -> 01101. Convert each binary sequence back into its number using the table above.

Using the binary from the middle screen of the module, for each bit, if the bit equals 1, then take the number at that position and do the following to get a new number:  $27 - \# = \#$ . Ex: 101100: 5 14 8 2 17 21  $\rightarrow$  22 14 19 25 17 21.

Finally turn each number back into a letter by treating the number as its alphanumeric position.

### Step 5: Base Caesar Cipher

On page 2 of the module, the bottom screen shows a number. However this number is not in base 10.

To figure out which base the number is in, take the sum of the alphanumeric positions of the letters of the encrypted word you have so far (A = 1, B = 2, ... Z = 26). Then modulo 8 the sum (subtract 8 to the sum until the number is between 0 - 7), then add 2. The resulting number is the base of the number.

To convert the number to base 10 follow the steps below:

Step 1: Above each of the digits in your number, list the power of the base that the digit represents. Start at 0 on the right and increment by 1 as you go left for each digit.

Step 2: Multiply each digit by the power of the base.

Step 3: Add all the numbers together to get your base 10 number.

EX: 132, Base 5

$$5^2 \ 5^1 \ 5^0$$

$$1 \ 3 \ 2$$

$$5^2 * 1 = 25$$

$$5^1 * 3 = 15$$

$$5^0 * 2 = 2$$

$$25 + 15 + 2 = 42$$

132 in base 5 is equal to 42 in base 10.

After converting the number to base 10, add the number to each letter of the encrypted word to get a new encrypted word.

EX:

$$A + 12 = 1 + 12 = 13 = M$$

$$E + 21 = 5 + 21 = 26 = Z$$

$$G + 24 = 7 + 24 = 31 - 26 = 5 = E$$

$$H + 123 = 8 + 123 = 131 - 26 = 105 - 26 = 79 - 26 = 53 - 26 = 27 - 26 = 1 = A$$

### Step 6: Enigma Cipher

On page 3 of the module, you will see a configuration of the rotors/reflector, the rotors setup below that, and a plugboard setup on the bottom.

### Step 6A: Configuration of the Rotors/Reflector/Plugboard

The screen at the top shows what type of rotors are used, the order they are in, and which reflector is used. Use the correct rotor charts and correct reflector chart to use to create an Enigma Decryptor.

They are read in this order: Reflector-Bottom Rotor-Middle Rotor-Top Rotor. Above the top rotor, you will type A-Z to use as the plugboard.

Use the schematic at the bottom to help you create the Enigma Decryptor.

The rotors below the screen shows what letter each one is at. Shift the letters until the bottom left letter is equal to the letter on the rotor.

For each pair of letters on the plugboard setup, switch the 2 letters positions on your plugboard.

### Rotor I

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

### Rotor II

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

### Rotor III

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

### Rotor IV

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

### Rotor V

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

### Rotor VI

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

### Rotor VII

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

## Rotor VIII

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

## Reflector A

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

## Reflector B

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

## Reflector C

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

## Enigma Schematic

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

**TOP ROTOR/RIGHT ROTOR**

**MIDDLE ROTOR**

**BOTTOM ROTOR/LEFT ROTOR**

**REFLECTOR**

## Step 6B: Rotor Turning Mechanics

On an enigma machine, everytime a letter is pressed, the rotors turn then a light lits up a single letter. Unfortunately we don't have an enigma machine with these wirings so you have to act like one. The first thing you have to do is turn rotors based on the rules below then decrypt the letter. This next section talks about how rotor turning mechanics work.

You will notice a couple letters on the bottom row of the rotors have \* next to them. Depending on which rotor it's on will have different effects:

- If the asterisk is at the leftmost edge of the middle rotor, all 3 rotors will turn
- Otherwise, if the asterisk is at the left most edge of the right/top rotor, both the middle and top/right rotor will turn.
- Otherwise, only the right/top rotor will turn
- Each turn only goes up 1 step on the rotor (Ex: A → B, G → H, Z → A, etc.)

### Step 6C: Using the Enigma Decryptor

- 1: Take the letter of your word and find it on the plugboard row of the decryptor.
- 2: Go straight down to the top row of the top rotor to receive a new letter.
- 3: Find the new letter in the bottom row of the top rotor.
- 4: Go straight down to the top row of the middle rotor to receive a new letter.
- 5: Find the new letter in the bottom row of the middle rotor.
- 6: Go straight down to the top row of the bottom rotor to receive a new letter.
- 7: Find the new letter in the bottom row of the bottom rotor.
- 8: Go straight down to the top row of the reflector to receive a new letter.
- 9: Find the new letter in the bottom row of the reflector.
- 10: Go straight up to the bottom row of the bottom rotor to receive a new letter.
- 11: Find the new letter in the top row of the bottom rotor.
- 12: Go straight up to the bottom row of the middle rotor to receive a new letter.
- 13: Find the new letter in the top row of the middle rotor.
- 14: Go straight up to the bottom row of the top rotor to receive a new letter.
- 15: Find the new letter in the top row of the top rotor.
- 16: Go straight up to the plugboard row to receive your decrypted letter.
- The example below uses I as the letter which will decrypt it to F.

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

Repeat steps 6B and 6C for each letter of your word to get a new encrypted word.

### Step 7: Railfence Playfair Cipher

On page 4 of the module, you will see 3 words, 1 on each screen.

To obtain the key, follow the steps below:

- 1. Use the number of batteries to determine the order of the words:

0 BAT: Top, Middle, Bottom  
 1 BAT: Top, Bottom, Middle  
 2 BAT: Middle, Top, Bottom  
 3 BAT: Middle, Bottom, Top  
 4 BAT: Bottom, Top, Middle  
 5+ BAT: Bottom, Middle, Top

- 2. Determine the number of rows the Railfence is by using this equation: (# OF PORTS % 5) + 2
- 3. Start zig-zagging the letters for that many rows going down first, then back up, left to right.
- 4. Take each letter in reading order to get the new arrangement of letters.
- 5. Take the entire alphabet and place it at the end of the string you made.
- 6. Replace any Js with Is.
- 7. Each letter must occur only once. If there are any duplicates, remove the 2nd or more occurrence, never remove the 1st occurrence.

Below is an example using Sand, Jowls, and Double as the 3 words, with 2 batteries and 4 ports:

SAND, JOWLS, DOUBLE -> JOWLS, SAND, DOUBLE

$$(4 \% 5) + 2 = 6 \text{ rows}$$

J	0
O	D U

W D B  
 L N L  
 S A E  
 S

JOWLSSANDDOUBLE -> JOODUWDBLNLSAES

JOODUWDBLNLSAES + ABCDEFGHIJKLMNOPQRSTUVWXYZ ->

JOODUWDBLNLSAESABCDEFGHIJKLMNOPQRSTUVWXYZ

Replace Js with Is -> IOODUWDBLNLSAESABCDEFGHIJKLMNOPQRSTUVWXYZ

Remove Duplicates -> IODUWBLNAESCFGHKMPQRTVXYZ

Once you have the 25 length string, create a 5x5 matrix of letters.

Replace any Js from your encrypted word to Is and split the word into character pairs. For each pair:

- If the 2 letters are exactly the same, keep them as is.
- Otherwise, if the letters appear on the same row of your matrix, replace them with the letters to their immediate left respectively, wrapping around to the right side of the row.
- Otherwise, if the letters are on the same column of your matrix, replace them with the letters immediately above, wrapping to the bottom.
- Otherwise, replace each of them with the letter on the same row but in the column of the other letter in the original pair.

### Step 8: Mechanical Cipher

On page 5 of the module, the top screen shows another pigpen cipher word. Use step 1 to decipher it.

Use the now deciphered pigpen word for the rows and use the word you have been decrypting as the columns. For each letter of each word, use the table below to get a new letter. Do this for each letter to get your decrypted word.

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

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

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.