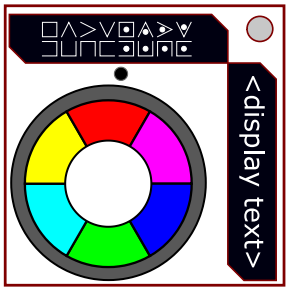
On the Subject of Unfair's Cruel Revenge



He made two versions of Unfair's Revenge because he wanted something more unfair than just the base idea... Was it unfair enough in the first place?

To distinguish this from Unfair Cipher and Unfair's Revenge, the 2 displays on this module are identical with one of them being rotated. The display on top shows the encrypted message. There's also a strip of LEDs underneath which will light up to show the current stage the defuser is on.

The display on the right can be clicked to cycle between showing the Module ID, in white, strikes the module is keeping track of, in red typically, and the extra keys. The Module ID and the strike counter are either shown in fixed or broken Roman numerals (VII, IX, IIII, ...), or in Arabic form. (1, 2, 3, 5, ...) Refer to Roman Art (Roman%20Art%20censored.html) for a reference to Broken and Fixed Roman Numerals. Zero (0) in Fixed/Broken Roman Numerals will be shown as literally nothing on the module and "0" in Arabic form.

For all operations involving STRIKES, always refer to the number on the second screen on the module itself.

The module encrypts a string of six distant three-letter-long instructions with different ciphers, using different **keys** for each. Enter the correct combination of inputs to disarm the module.

ALL ciphers referring to the alphabet refers to the A1Z26 standard for each letter unless stated otherwise. Alphabetical order is ALSO modified for the ciphers!

- The basic order of the given encrypted text is the following: **Original -> Message Splitting (Depending on Time of Activation) -> 1-4x Ciphers For Each -> Concatenated -> Pigpen Ciphered.** Reverse the order to obtain the **original** instruction string.

The next pages will go over instruction on how to decrypt the latest version of Unfair's Cruel Revenge. If some information is missing on the module, the defuser may have enabled Legacy Unfair's Cruel Revenge. Check the legacy manual on how to disarm that. You will know if you have legacy Unfair's Cruel Revenge enabled if the following is true: The 4th page is empty except with "=LEGACY=" at the bottom; Page 3 on the module has 2 sets of information dashed out.

Solving — Step 0: Understanding The Extra Screen

The extra screen has a nifty indicator on the side that is used to indicate what page you are on currently. The page the defuser is currently on is marked in white with the first LED on the top denoting the first page.
There are four pages that the defuser can cycle to by selecting the top or bottom halves of the screen to cycle the pages up or down respectively. (down going to the next page, up going to the previous page.)
The first page will show the Module ID, which is shown in Broken or Fixed Roman Numerals or in Arabic Numerals; the second page will show the Strike Counter, which is shown in Broken or Fixed Roman Numerals or in Arabic Numerals. In addition, the second page will have its text colored differently depending on what mode it has started in.
The third page on the other hand consists of the following in no particular order:

- Up to 8 numbers when rearranged form consecutive numbers
- A falsely selected word from Word Search (Word%20Search.html)
- 12 Pigpen encrypted letters for Four Square Cipher
- 7 base-24 digits used for obtaining Key A
- And a decrypted word from an older version of Ultimate Cipher (Ultimate%20Cipher.html).

The positioning of those numbers, the falsely selected word, and the pigpen encrypted letters will vary and may be used to determine how the cipher operates but the base 24 digits and the Ultimate Cipher word will always be in the same position.
The fourth page consists of the following in this specific order:

- 18 pigpen letters used for encrypting any (10th letters) for Playfair/Four Square Ciphers for the base message
- 1 to 8 characters used to determine what ciphers were used, surrounded by "=". For the context in the manual, they are referred to as hexadecimal cipher digits.

An example of the extra screen is shown here. Here it is showing page 3 with the following in no particular order, the falsely selected word, the consecutive numbers, 12 Pigpen encoded letters, the base-24 number, and the Ultimate Cipher word.

Solving — Step 0.5: Prepping The Keys

You are going to need to obtain these keys and values in order use the ciphers later on.

Key A

1. Start 6 base-24 digits on the module for key A. You can find this to the left of the Ultimate Cipher decrypted word.
2. Convert this base-24 number into **hexadecimal.** You can do this by converting the base-24 value into base-10 and then converting the base-10 value into hexadecimal. Refer to *Appendix HexDex* for instructions to convert base-10 into hexadecimal and *Appendix Base-24 Conversion* for converting base-24 into base-10.
3. Now read the string of hexadecimal digits as a string of decimal digits and letters. Going from left to right, for every digit:
    - If the digit is followed by another digit and they form a number in the range 10-26, convert the pair into its alphabetical equivalent.
    - Otherwise, convert the single digit into its alphabetical equivalent, or skip it if it is a zero.
4. Transform the Module ID, (1 + the number of port plates), and (2 + the number of battery holders) into their alphabetical equivalents, separately, using step 4 if any of these are greater than 26.
5. Append these characters together and then at the end of the result of the previous conversion.
6. **This is Key A.**

Key B

Obtain Key B from the following table using the month and day of the week of when this module was activated:

		Month											
		Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Day	Mon	ALPH	ONE	ABCD	AEI	PLAY	JAKK	FRLA	ZEKN	FIZZ	HEND	CLUT	SCG
	Tue	BETA	TWO	EFGH	OUY	HIDE	MCDU	VIRE	ELIA	TIMW	ACRY	MAGE	BASH
	Wed	CHAR	THRE	IJKL	WBC	SECR	EOTA	IONL	REXK	MOON	ONYX	SPAR	MOCK
	Thu	DELT	FOUR	MNOP	DFG	CIPH	CAIT	LEGN	RIVE	TAOO	SAMD	KONQ	BRIN
	Fri	ECHO	FIVE	QRST	HJK	FAIL	MARA	WILL	TRAI	LUPO	ELUM	FLAM	KANE
	Sat	FOXT	SIX	UVWX	LMN	PART	WARI	SKIP	NANT	LUMB	FLUS	MOMO	HEXI
	Sun	GOLF	SEVN	YZAB	PQR	BECO	PIGD	ETRS	GRYB	CATN	ASIM	MITT	PERK

Key C

Sum up the value of ALL the false rules in Alphabetize (Alphabetize.html), as if there are no strikes, no solved modules on the bomb, which is determined by the position in the table, 1 being the top-most row. Then take the average of the sum. If this result is not an integer, use the 15th row on that manual as Key C, otherwise count that many rows from the top and use that as Key C.

Value X Table

Condition	Operation
For each BOB, CAR, or CLR indicator:	+1 if lit, -1 if unlit
For each FRK, FRQ, MSA, or NSA indicator:	+2 if lit, -2 if unlit
For each SIG, SND, or TRN indicator:	+3 if lit, -3 if unlit
For the number of batteries:	+4 for odd, -4 for even
There are port plates with parallel port:	+5 each, -4 if paired with serial port
There are port plates with DVI-D:	-5 each, +4 if paired with Stereo RCA

Start with 0 and perform all operations from the table above in this section for each condition. If the value is negative, make it positive. This will be referred to as X for decrypting.

Value A Table

Condition	Operation
For every **port type**	−2
For every **port plate**	+1
For every **consonant** in the serial number	+1
For every **vowel** in the serial number	−2
For every **lit** indicator	+2
For every **unlit** indicator	−2
For every **battery**	−1
No batteries	+10
No ports	×2
31 or more modules	÷2

Start with 0 and perform all operations in the following table for each condition from top to bottom. This will be referred to as Value A for decrypting. Drop any remainders and/or decimals when using the division operation. I.E, if you get −1.5 after division, turn −1.5 into −1 instead.

Solving — Step 1: Determining The Selected Ciphers

Countdown Timer Upon Activation	Ciphers Used	Hexadecimal Cipher Length
30:00+†	1 shared, 2x 3 ciphers	6
22:30 - 29:59*	2x 2 ciphers	4
15:00 - 22:29	3 ciphers	3
7:30 - 14:59	2 ciphers	2
0:00 - 7:29	1 cipher	1

Examine the countdown timer when the bomb has activated. Not to be confused with starting time, which is obtained when the module is loaded in; use that information in the first column and find the cell that fits with that time. Now use that row corresponding to the cell obtained from that time to determine what ciphers are used.

† Use THIS row if the bomb started in Zen/Training Mode. This takes precedence over activation time. You will know when to use this when the strike text's color is **CYAN** and NOT red.

* Use THIS row if the bomb started in Time Mode. This takes precedence over activation time. You will know when to use this when the strike text's color is **ORANGE** and NOT red.

Note: The previous section can be cheated since the length of the hexadecimal cipher number is VERY predictable and easy to determine. Use ONLY the last 2 columns on this table to determine it.

If your row obtained from the table contains "#x" for the ciphers that are used, this denotes that the instructions were split and encoded separately before being displayed in Pigpen Cipher as 1 entire message.

If you are splitting this into 2 parts, perform a 10-8 split ("ABCDEFGHIJ", "KLMNOPQR") if Blue and Yellow are both on the upper/lower halves of the module or an 8-10 split ("ABCDEFGH", "IJKLMNOPQR") otherwise. Do the same action with the substitution letters.

If the defuser has colorblind mode enabled for this module, hovering over the colored button will show the color of that given button for that given position on the top screen.

Solving — Step 1.5: Decoding the Selected Ciphers

Encryption Type	Character of Reference
Substitution Playfair Cipher (Key A)	0
Substitution Playfair Cipher (Key B)	1
Substitution Playfair Cipher (Key C)	2
Caesar Cipher (Value A)	3
ROT13 Cipher	4
Affine Cipher (Value X)	5
Atbash Cipher	6
Basic Columnar Transposition	7
Myszkowski Transposition	8
Anagram Shuffler	9
Scytale Transposition	A
Autokey Mechanical Cipher	B
Substitution Four Square Cipher (Keys ?)	C
Redefence Transposition	D
Monoalphabetic Substitution	E
Running Key Alberti Cipher	F

The table above shows all possible ciphers that can be used on Unfair's Cruel Revenge. The original set of instructions were encrypted by the ciphers determined by the hexadecimal number, from left to right for each set, and then encrypted with Pigpen Cipher to be displayed on the module after combining the encrypted messages together. The expert will need to grab those ciphers that are used on this module, and then decrypt them by reversing the procedure. For example, if the determined ciphers in the list are ROT13 Cipher, Atbash Cipher, Autokey Mechanical Cipher, Anagram Shuffler, and Scytale Transposition, the order to decrypt this is Scytale Transposition, Anagram Shuffler, Autokey Mechanical Cipher, Atbash Cipher, ROT13 Cipher in that order.

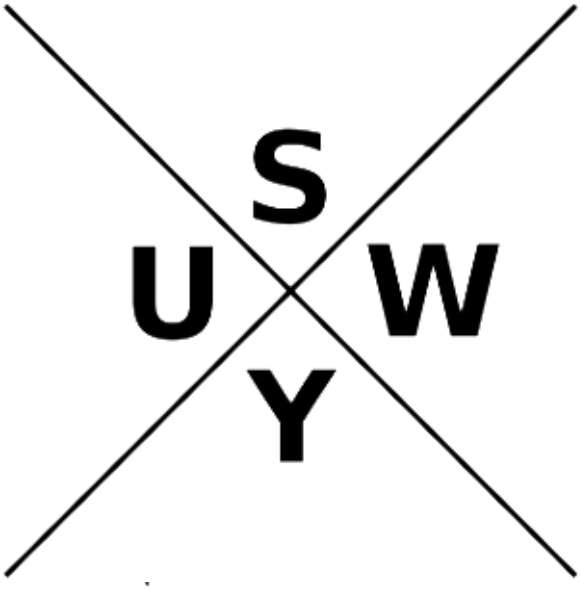
To do so split the hexadecimal characters into equal parts and decode each of them to get the ciphers used for each set, where the left-most set of ciphers are used for the first set of messages, the right-most set of ciphers are used for the last set of messages, and so on.

Solving — Step 2: Pigpen Cipher

Convert the symbols on the top screen into letters using the chart below.

A	C	E
G	I	K
M	O	Q

B	D	F
H	J	L
N	P	R



Solving — Step 3: Modifying the Base Alphabet

Did he put a "Blue Arrows" in "Unfair's Revenge?" Don't tell me he did...

You will need to modify the starting alphabet in order to use the ciphers and transpositions on the next set of pages when the modified alphabet is needed. To get the modified alphabet:

1. Start the alphabet with "ABCDEFGHIJKLMNOPQRSTUVWXYZ".
2. Shift the entire alphabet to the right [1 + the last digit of the serial number (10 if none)] times.
3. If there are any letters in the serial number, move the last letter of the serial number to the front of the alphabet. If that letter is already in the front, move it to the back instead.
4. Then, perform the extra modifications from the table below, top to bottom. Your alphabet for decrypting will be the string after using the table on both pages. Conditions referred from the table are labeled from top to bottom, starting on 1 with the top-most row, on this page.

Condition	Action
Exactly all of these: Lit BOB, no batteries, no port plates, no unlit indicators, serial number contains a vowel	Throw away your current string from this point and use the starting alphabet instead for decrypting. Skip the rest of the conditions from this table.
Lit BOB is present	Reverse the entire string.
Odd number of battery holders	Move the vowels ("A", "E", "I", "O", "U") to the back of the string, keeping the order they appeared. If "W" is also in the serial number, move that letter as well in respect with the other vowels.
Number of batteries is 3n	Take the letters where the position in the string (the first letter in the string being position 1) has exactly 3 or 4 distinct factors (including 1 and itself), reverse that set, and append it to the back of the string.
"Green Arrows", "The Sphere", or "Yellow Arrows" are present	Put "LAZYDOG" at the very front of the string and then remove duplicate letters afterwards.
Unfair's Revenge is present	Reverse the 2nd half of the string, and then put "THEQUICK" at the very back of the string, in that specific mentioned order.

Solving — Step 3: Modifying the Base Alphabet (Cont.)

Condition	Action
DVI-D port is present	Reverse the first half of the string.
Stereo RCA port is NOT present	Move letters R, C, and A to the very back of the string, in that specific mentioned order.
Duplicates of Unfair's Cruel Revenge are present	Shift the entire alphabet to the right [10 times (the number of Unfair's Cruel Revenge modules, minus 1)] times.
An odd number of conditions were met (upon reaching this condition)	Undo the action that was performed from the last condition that was met.
At least 1 empty port plate is present	Split the alphabet into 2 halves where the first half contains the letters whose position in the string (the first letter in the string being position 1) is divisible by 6. Shift the other half to the right 6 times, then combine the halves together with the shorter string being first.
Who's on First or What's on Second is present AND the 11th condition is NOT met	Move all of the letters between "U" and "H" to the very front of the string, excluding "U" and "H" respectively. If "U" and "H" are adjacent, move those to the front of the string instead, keeping the order they appeared.
Blue Arrows is present and any previous condition(s) were met (upon reaching this condition)	Undo the action that was performed from the last condition that was met. However, if the last condition met was the 10th condition apply the action from the 12th condition.
No other conditions were met	Perform a ROT13 cipher with your current string using the English Alphabet, then using the first digit of the serial number, perform the action corresponding to the (n+1)th condition whose action does NOT undo or discard the string. In the case of no digits, apply the action of the 3rd condition (from the table). **F**

Solving — Step ?: Affine Cipher

For each letter in the plain text:

- The alphabetic position of that letter is multiplied by (2X + 1).
- 26 is subtracted from the product until it falls within the range [1, 26].
- This is the alphabetic position of the encrypted letter.

To decrypt, add 26 to the alphabetical position of the encrypted letter until it is divisible by (2X + 1), then divide it by (2X + 1) to get the alphabetical position of the unencrypted letter. Repeat until you have your original message.

The table underneath can be used to quickly decrypt each letter for Affine Cipher if needed. The table uses the Standard English Alphabet order however the alphabet used on the module may be different. X = 0 denotes to the first row in the table and the decrypted letter, X = 1 for the 2nd row for the encrypted letter, X = 2 for the 3rd row, etc.

Edit the field provided to obtain the affine table for the alphabet being used. This must contain exactly 26 distinct letters.

Modifiable Affine Encryption Table																ABCDEFGHIJKLMNOPQRSTUVWXYZ									
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
C	F	I	L	O	R	U	X	A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z
E	J	O	T	Y	D	I	N	S	X	C	H	M	R	W	B	G	L	Q	V	A	F	K	P	U	Z
G	N	U	B	I	P	W	D	K	R	Y	F	M	T	A	H	O	V	C	J	Q	X	E	L	S	Z
I	R	A	J	S	B	K	T	C	L	U	D	M	V	E	N	W	F	O	X	G	P	Y	H	Q	Z
K	V	G	R	C	N	Y	J	U	F	Q	B	M	X	I	T	E	P	A	L	W	H	S	D	O	Z
The message to decrypt would result in very ambiguous conditions if using X = 6.																									
O	D	S	H	W	L	A	P	E	T	I	X	M	B	Q	F	U	J	Y	N	C	R	G	V	K	Z
Q	H	Y	P	G	X	O	F	W	N	E	V	M	D	U	L	C	T	K	B	S	J	A	R	I	Z
S	L	E	X	Q	J	C	V	O	H	A	T	M	F	Y	R	K	D	W	P	I	B	U	N	G	Z
U	P	K	F	A	V	Q	L	G	B	W	R	M	H	C	X	S	N	I	D	Y	T	O	J	E	Z
W	T	Q	N	K	H	E	B	Y	V	S	P	M	J	G	D	A	X	U	R	O	L	I	F	C	Z
Y	X	W	V	U	T	S	R	Q	P	O	N	M	L	K	J	I	H	G	F	E	D	C	B	A	Z

Solving — Step ?: Atbash Cipher

Each letter is encrypted to a new letter whose alphabetical position is (27 − P), where P is the alphabetical position of the unencrypted letter.
To decrypt simply get the letter whose alphabetical position is (27 − E), where E is the alphabetical position of the encrypted letter.

Solving — Step ?: Substitution Playfair Cipher (Key X)

- Omit any (10th letters) in your keyword.
- Create a 5×5 matrix of letters. Start with your **keyword (Key X in this case)** and fill the rest with the unused letters of the alphabet from step 3, omitting the (10th letter). Each letter must occur only **once** in the matrix, so only add the first occurrence.
- Split the **message** into character pairs. If you cannot form a pair, **do not encrypt/decrypt that letter**. If there are any (10th letter)s in the pair change them into the letter corresponding to the substitution sequence. Change those back to (10th letter)s after decrypting. For each pair while decrypting:
  - If the letters are exactly identical, do not modify them at all.
  - 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 other side of the row if necessary.
  - If the letters are on the same column of your matrix, replace them with the letters immediately above, wrapping to the other side of the column if necessary.
  - If the letters are on different rows and columns, replace each of them with the letter on the same row but in the column of the other letter in the original pair.
- Concatenate the pairs to obtain your decrypted section, making sure any letters that were previously (10th letter)s are converted back into (10th letter)s.

Solving — Step ?: Caesar Cipher

To decrypt from Caesar Cipher, shift every letter on the screen forwards by this many letters in the alphabet being used if the offset is negative, backwards if the offset is positive. Wrap back to the other side of the alphabet if you have to go backwards from the first letter in the modified alphabet or forwards from the last letter in the modified alphabet.

Solving — Step ?: ROT13 Cipher

Each letter is encrypted by using Caesar Cipher with a key of 13 on the given alphabet, wrapping around to the first letter if needed.

To decrypt, simply do Caesar Cipher with a key of 13.

Solving — Step ?: Basic Columnar Transposition

The extra key will contain random numbers when rearranged form consecutive numbers. These have been used to encrypt the instructions.

To decrypt, create dashes equal to the length of your encrypted message, and underneath the numbers displayed.

Example with the number key "316245" and 18 letters:

3	1	6	2	4	5
-	-	-	-	-	-
-	-	-	-	-	-
-	-	-	-	-	-

Example with the number key "415236" and 15 letters:

3	1	6	2	4	5
-	-	-	-	-	-
-	-	-	-	-	-
-	-	-			

Then fill each column starting on 1 with the first letters in your encrypted message, then the next set on 2, until you have replaced all of the dashes.

Now read the message underneath the numbers in reading order to get your decrypted message.

An example to decrypt to "ANSWERING CANNOT BE AMBIGUOUS" from "ACMNESSNIRTOEOUWNGIBUNABGA" in 3 rows with the key 183654729 can be demonstrated here.

1	8	3	6	5	4	7	2	9
-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	-
-	-	-	-	-	-	-	-	

Initial setup with key "183654729", 26 letters
May differ from original module

1	8	3	6	5	4	7	2	9
A	-	-	-	-	-	-	-	-
C	-	-	-	-	-	-	-	-
M	-	-	-	-	-	-	-	

Replace dashes under the column marked "1" with "ACM"

1	8	3	6	5	4	7	2	9
A	-	-	-	-	-	-	N	-
C	-	-	-	-	-	-	E	-
M	-	-	-	-	-	-	S	

Replace dashes under the column marked "2" with "NES"

1	8	3	6	5	4	7	2	9
A	N	S	W	E	R	I	N	G
C	A	N	N	O	T	B	E	A
M	B	I	G	U	O	U	S	

Repeat with "3", "4", ...
Until all dashes have been replaced

Solving — Step ?: Myszkowski Transposition

These seem very familiar to the last one...

Keywords						
ARCHER	ATTACK	BANANA	BLASTS	BURSTS	BUTTON	CANNON
CALLER	CELLAR	DAMAGE	DEFUSE	DEVICE	KABOOM	LETTER
LOOPED	MORTAR	NAPALM	OTTAWA	PAPERS	POODLE	POOLED
RASHES	RECALL	ROBOTS	SAPPER	SHARES	SHEARS	WIRING

Take the sum of the serial number digits, modulo it by 28, add 1, and count that many words in reading order from the table to get your keyword, starting on "ARCHER".

The encryption process follows by splitting the unencrypted letters up so that each row is equal to or less than the length of the keyword. Using the keyword, the number string is obtained by assigning each letter in the keyword in alphabetical order, ties included, where 1 is a letter from the keyword that occurs earliest from the alphabet. The unencrypted letters are then read in ascending numerical order according to the number string obtained earlier, from left to right, top to bottom. Refer to this (https://en.wikipedia.org/wiki/Transposition_cipher) for clarification.

To decrypt, place each letter underneath the number string obtained, in ascending numerical order. In the case of duplicate numbers in the number string, place them from left to right, top to bottom for the current duplicate number, until each have been filled. Then read the message in reading order to get the decrypted text. The example of Myszkowski Transposition being used is demonstrated underneath.

Example: Myszkowski Transposition

The plain text used for this example is "BOBRAN FASTER THANON EHORSE." The keyword used is "PAPERS" using the Modern English Alphabet for encrypting. The number key obtained from this from "PAPERS" is "313245." The text when encrypted reads "OAHH RTNR BBFS TAEO AEOS NRNE." Spaces are provided in the quotes for readability for decrypting and encrypting.

P	A	P	E	R	S
3	1	3	2	4	5

3	1	3	2	4	5
B	O	B	R	A	N
F	A	S	T	E	R
T	H	A	N	O	N
E	H	O	R	S	E

Solving — Step ?: Scytale Transposition

1. Add 2 to (the number of ports on the bomb modulo 4); this is how many rows you will need to make.
2. Create dashes that match the length of the string, and to match the height of the theoretical cylinder. The dashes should start on the top-left and repeat every X letters, based on the height of the cylinder.

Example, with 3 rows and 11 letters:

-			-			-			-	
	-			-			-			-
		-			-			-		

3. Fill each dash in reading order with each letter in the string you have encrypted.
4. The read each letter like reading a ribbon wrapped around the cylinder.
5. This results in your <u>decrypted</u> string for Scytale Transposition.

An example to decrypt to "ORANGEJUICE" from "ONJCRGUEAEI" in 3 rows can be demonstrated here.

O			N			J			C	
	R			G			U			E
		A			E			I		

Solving — Step ?: Redefence Transposition

As if Railfence wasn't easy enough.

You will need to use the Columnar Transposition key from the extra key in order to decrypt this.

Create dashes in a zig-zag formation so that the length is equal to the length of the encrypted text and the height is equal to the number of numbers in the given key.

Example, with 3 rows and 11 letters:

-				-				-		
	-		-		-		-		-	
		-				-				-

Now insert numbers to the left of the formation you made where the top-most row takes the 1st number, the 2nd top-most row takes the 2nd, etc. until each row has a number assigned.

To <u>decrypt:</u>

1. Replace as many dashes on with the first set of letters in the encrypted string on the row with the smallest number.
2. Repeat the previous step with the 2nd, 3rd, ... smallest numbers using the next set of letters until each dash has been replaced.
3. Read the letters on the zig-zag formation you made to get your decrypted string.

An example to decrypt to "FOURHUNDRED" from "FHRUNDORUDE" in 3 rows with the key 132 can be demonstrated here.

1	-				-				-		
3		-		-		-		-		-	
2			-				-				-

Initial setup with key "132", 11 letters

1	F				H				R		
3		-		-		-		-		-	
2			-				-				-

Filled in dashes on the row marked "1"

1	F				H				R		
3		-		-		-		-		-	
2			U				N				D

Filled in dashes on the row marked "2"

1	F				H				R		
3		O		R		U		D		E	
2			U				N				D

Filled in dashes on the row marked "3", decrypted upon reading zig-zag way

Solving — Step ?: Autokey Mechanical Cipher

You're telling [at most] 18 letters for 1 cipher!? That's completely out of his mind!

The portion of the extra key will consist of a falsely selected word from the module, Word Search (Word%20Search.html). The actual word used for encrypting is the word in the same cell as the falsely selected word, E.G if the falsely selected word is "TEST", the word used for encrypting is "JINX."

Part of the plain text is added to the right of the base key to form a length equivalent to the length of the plain text.

Then the module is encrypted from a theoretical table called *Tabula Recta*. Each letter of the plain text is used for the column, and each letter of the key is used for the row.

However, the row used on the next page is numbers instead of letters. How did the module encrypt it? The following instructions were left:

1. Take the alphabetical position of each letter in the keyword and pair these numbers with each of the letters in the plain text.
2. Obtain the intersection of the first letter/number pair to obtain the encrypted letter.
3. Repeat for the rest of the letter/number pairs until you have an encrypted message.

To decrypt:

1. Start with the first X characters of the encrypted string where X is the length of the keyword.
2. Decrypt this set by undoing the procedure mentioned on this page to get the first set of letters that was appended to the keyword.
3. Repeat this with the next set of letters in your encrypted string until you have decrypted your entire encrypted string.

An example of the decryption procedure for decrypting to get "APPLES" with the keyword "ATE" can be shown here. The alphabet used in this example is the Standard English Alphabet.

?	?	?	?	?	?
A	**T**	**E**	**?**	**?**	**?**
T	X	C	D	H	C

Initial Setup, may differ from module

A	P	P	?	?	?
A	**T**	**E**	**?**	**?**	**?**
T	X	C	D	H	C

Decrypt letters from keyword provided

A	P	P	?	?	?
A	**T**	**E**	**A**	**P**	**P**
T	X	C	D	H	C

Add some decrypted text to keyword

A	P	P	L	E	S
A	**T**	**E**	**A**	**P**	**P**
T	X	C	D	H	C

Decrypt Section → Result of decrypting

Go here (https://crypto.interactive-maths.com/autokey-cipher.html) for information about Autokey cipher.

Autokey Mechanical Cipher's *Tabula Recta*

	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	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L
2	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O
3	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F
4	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A
5	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E
6	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T
7	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G
8	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D
9	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H
10	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I
11	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M
12	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J
13	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y
14	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P
15	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N
16	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q
17	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R
18	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W
19	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V
20	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S
21	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X
22	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U
23	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C
24	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z
25	H	F	V	G	L	T	J	O	N	X	A	K	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B
26	I	P	C	Z	D	W	U	S	R	Q	M	Y	E	B	H	F	V	G	L	T	J	O	N	X	A	K

Solving — Step ?: Anagram Shuffler

Did you know that "Orange" is an anagram of "A Goner?"

Anagrams					
TAMERS	STREAM	MASTER	ARM SET	MRS TEA	MR SEAT
BARELY	BARLEY	BLEARY	LAB RYE	A BERYL	ALB RYE
RUDEST	DUSTER	RUSTED	ED RUST	EDS RUT	DUST RE
IDEALS	SAILED	LADIES	A SLIDE	DEAL IS	SEA LID

Use 2 or 4 if the pigpen set is at the top on the extra key screen, otherwise use 1 or 3. Use the smaller number if the Columnar Transposition key is to the left of the falsely selected word used for Autokey Cipher, otherwise use the larger number. This number is the row number used for this table.

Then count the anagrams in that row from left to right, by the number of steps it takes to reach to Green, starting on the NW button and going CW if the current button is not Green until landing on Green, plus 1. That will be the base key for the unencrypted string.

If the base key consists of 2 words, swap them if the serial number does not contain a vowel (A, E, I, O, U).

Finally, count the anagrams in the same row from left to right, by the number of steps it takes to reach to Magenta, starting on the NW button and going CW if the current button is not Magenta until landing on Magenta, plus 1. That will be the encryption key.

If the encryption key consists of 2 words, swap them if there are an odd number of battery holders on the bomb.

To decrypt, create dashes in reading order in respect to the length of the base key. Now copy the pattern of dashes underneath in relation to each letter in the encryption key. Replace the dashes with the letters in your encrypted message under your encryption key in reading order. Then copy the columns in respect to encryption key to the base key. Obtain the letters in reading order to obtain your decrypted string.

Anagram Shuffler Example

An example of Anagram Shuffler is used here, with the number of letters in the encrypted string not being divisible by the number of letters in the base and encryption key.

P	R	I	N	C	E
–	–	–	–	–	–
–	–	–	–	–	–
–	–	–	–		

P	R	I	N	C	E
A	F	A	I	N	T
S	O	U	N	D	H
E	A	R	D		

P	I	N	C	E	R
–	–	–	–	–	–
–	–	–	–	–	–
–	–	–			–

P	I	N	C	E	R
A	A	I	N	T	F
S	U	N	D	H	O
E	R	D			A

Solving — Step ?: Substitution Four Square Cipher (Keys ?)

I think he ran out of ideas for potential reasonable ciphers.

The extra key consists of 12 random pigpen letters, which are used for square D. Decrypt this by using step 2 from the manual. For the other 3 keys:

1. Obtain keys A, B, and C by going through the instructions in **Prepping The Keys.**
2. Omit the 10th letter in the alphabet for each key, then remove duplicate letters and fill in the rest of the alphabet if necessary at the end of each key.
3. Create 4 5x5 squares in that regard.
4. Rearrange the squares into the following: A on the top-left, B on the top-right, C on the bottom-left, D on the bottom-right. Refer to the table for this step for the order.

A	B
C	D

5. Convert any (10th letters) in your encrypted message into the letters in the substitution sequence from their respective positions.
6. Now refer to Orange Cipher (Orange%20Cipher.html) for the next step. This page will repeat the procedure from Step 3's Orange Cipher if the link is broken.
7. To decrypt, split the encrypted string into pairs. Then for each pair:
    - Grab the row and column of the 1st letter in the pair from the TR square.
    - Grab the row and column of the 2nd letter in the pair from the BL square.
    - Use the row position of the 1st letter and the column position of the 2nd letter to get your 1st decrypted letter in the TL square for that pair.
    - Use the column position of the 1st letter and the row position of the 2nd letter to get your 2nd decrypted letter in the BR square for that pair.
8. Concatenate the decrypted pairs together. Then if any of the letters were previously (10th letter)s, replace them with (10th letter)s. This results in your decrypted string.

Solving — Step ?: Monoalphabetic Substitution:

It's actually this easy. But without the key? Lots of guessing and checking. That's how the experts cracked that one code.

Start with the Ultimate Cipher word and remove any duplicates. Now examine the modified alphabet and remove ALL letters that are in your Ultimate Cipher word. If the NE button is yellow, place the result of your modified alphabet at the start of your Ultimate Cipher word. (I.E: "CABLERDFGHIJKMNOPQSTUVWXYZ") Otherwise, place your modified alphabet at the end of your Ultimate Cipher word. (I.E: "DFGHIJKMNOPQSTUVWXYZCABLER")

To decrypt, you will need to place this string, "ABCDEFGHIJKLMNOPQRSTUVWXYZ", at the top in this specific order, and then place the key underneath that was used to encrypt your message. Now examine the first letter in the encrypted message in the key. The letter above is the result of your decryption. Repeat for the other letters to get your decrypted string.

Example:

Say you're provided with this which was used to encrypt your message:

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

And the encrypted message was "RFDMOCNZCRQWCQGQFIQ."

You can start by examining the first letter in your encrypted message which is R. Examining the R in the encrypted row results in "U" when being decrypted.

Encrypted	R	F	D	M	O	C	N	Z	C	R	Q	W	C	Q	G	Q	F	I	Q
Decrypted	U																		

There is another "R" in that code so we can decrypt that letter in the same fashion as well.

Encrypted	R	F	D	M	O	C	N	Z	C	R	Q	W	C	Q	G	Q	F	I	Q
Decrypted	U									U									

Now we can examine the next letter in the code that was used to encrypt our message. Say we look at "Q" for this instance. This decrypts to "E" for these set of letters.

Encrypted	R	F	D	M	O	C	N	Z	C	R	Q	W	C	Q	G	Q	F	I	Q
Decrypted	U									U	E			E		E			E

Keep repeating this procedure with the other letters. This results with a decrypted text which reads "UNFAIRS CRUEL REVENGE."

Encrypted	R	F	D	M	O	C	N	Z	C	R	Q	W	C	Q	G	Q	F	I	Q
Decrypted	U	N	F	A	I	R	S	C	R	U	E	L	R	E	V	E	N	G	E

Solving — Step ?: Running Key Alberti Cipher

Alberti cipher was used to be one of the ciphers that was considered to be unbreakable before the documentations were publicly released in the 21st century. Now things got a lot more complicated.

This cipher may be complicated to master the first time around. You will need to use these paragraphs to obtain the key that encrypted your message.

The Alberti wheel, which you will create, consists of two parts, the stationary wheel or *Stabilis*, and the moving wheel or *Mobilis*. To create the wheel:

- Make the *Stabilis* with the English alphabet in order. Then to make the *Mobilis*, separate the modified alphabet by every other letter, to obtain two halves.
- If Red is diametrically opposite to Cyan, reverse the first half and swap those halves. Otherwise, reverse the second half. And then concatenate the halves together.
- Mark your anchor letter in your *Mobilis*, the first letter in the serial number, if there are any. Otherwise, mark "A" as your anchor letter instead.

Now take the first two letters in the twelve letter pigpen text and convert them into their alphabetical equivalents using step two from this manual provided.

Convert these into their positions in the modified alphabet. Start on the paragraph from the first number obtained where one or fourteen is the top paragraph.

Using the second number, count that many words from the paragraph you obtained earlier to obtain the start of your running key. Add the starting word.

- Ignore punctuation and font styles for each word you append onto your key. Repeat until the key is as long or longer than your encrypted message.
- Each relevant paragraph in this page is exactly twenty six words long. Continue to the first word of the next paragraph if you reach the end.

To decrypt your message, rotate the *Mobilis* so that the anchor letter is directly below the letter in the *Stabilis* for each letter in the key.

Examine the encrypted letter in your *Mobilis* to get your decrypted letter in your *Stabilis* in the same position. Repeat until you have your decrypted string.

When obtaining your key, if you reach the end of the last paragraph, wrap around to the first word of the first paragraph, upon reaching this.

Solving — Step ?: Alberti Cipher Example:

Say you're provided with this which was used to encrypt your message:

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

And the encrypted message was "BZFEXJFFCN" using the key "HAS SHE BEEN." The "!" on the table is denoted as the anchor letter on this wheel. The top row is the stationary tape, while the bottom row is the movable tape.

Let's start by finding an anchor point for the first letter, say "A". We would move the bottom tape so that our anchor letter, which is Z, is directly below A on the stationary tape.

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

Now we look at our encrypted letter above this to get our decrypted letter. For this instance we would look at "Z" in the moving wheel and above it is "A."

Encrypted	B	Z	F	E	X	J	F	F	C	N
Key	H	A	S	S	H	E	B	E	E	N
Decrypted		A								

Now we can move on to the next anchor letter to go for. Let's try "H". We would move the bottom tape so that our anchor letter is directly below H on the stationary tape.

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

Now we look at our encrypted letter above this to get our decrypted letter. For this instance we would look at "B" in the moving wheel and above it is "T."

Encrypted	B	Z	F	E	X	J	F	F	C	N
Key	H	A	S	S	H	E	B	E	E	N
Decrypted	T	A								

Since we have multiple letters that use the same key in that position, we can also account for the 5th letter in our encrypted string, which is "X."

Encrypted	B	Z	F	E	X	J	F	F	C	N
Key	H	A	S	S	H	E	B	E	E	N
Decrypted	T	A			I					

Keep repeating this procedure with the other letters. This results with a decrypted text which reads "TACH IM LOST"

Encrypted	B	Z	F	E	X	J	F	F	C	N
Key	H	A	S	S	H	E	B	E	E	N
Decrypted	T	A	C	H	I	M	L	O	S	T

Solving — Step 8: Executing the Instructions

If at this point the expert has at least 1 3-letter set not in the given list of instructions, the expert may need to redo the decryption process.

Tap the screen on the right to cycle between showing the module ID, the number of strikes obtained so far, which is not shown in white, or the extra keys.

Again, if the defuser has colorblind mode enabled for this module, hovering over the colored button will show the color of that given button for that given position on the top screen.

Instructions:

'%' refers to the modulo (remainder) operation.
Inner Center refers to the white button in the middle.
Outer Center refers to the gray circular frame around the colored buttons.

Refer to *Appendix PR1M3* for a list of prime numbers.

- **PCR:** Press the Red button.
- **PCG:** Press the Green button.
- **PCB:** Press the Blue button.
- **SCC:** Press the Cyan button.
- **SCM:** Press the Magenta button.
- **SCY:** Press the Yellow button.
- **SUB:** Press **Inner Center** when the seconds digits on the countdown timer match.
- **MOT:** Press **Outer Center** when the last digit on the seconds timer is $(m + c + (5 - s)) \% 10$, with m being the Module ID, c being the number of times a colored (R, G, B, C, M, Y) button has been pressed since the last strike on this module (or since the beginning if there are no strikes) and s being the current stage, starting with 1.
- **PRN:** Press **Inner Center** if (Module ID % 20) is a prime number; otherwise press **Outer Center.**
- **CHK:** Press **Outer Center** if (Module ID % 20) is a prime number; otherwise press **Inner Center.**
- **REP** or **EAT:** Repeat the last input, or press **Inner Center** if this is the first instruction. Ignore timing constraints.
- **STR** or **IKE:** Starting from the last colored button you pressed or Red if you have not pressed any colored buttons yet, count as many colored buttons counter-clockwise as there are strikes and press the resulting button. In the case of 0 strikes, press the starting button.
    - For these instructions, refer to the Strike Counter on the screen to the right of the module itself.

Instructions (Continued):

- **SKP:** Press **Inner Center.** Then press **Outer Center** and **skip the next instruction.** If this instruction is unable to skip the next instruction, or this is the very last instruction, only the **Inner Center** press is needed.
- **PVP** or **NXP:** Start from the last colored button you pressed (or the NW button if you have not pressed any yet). Go (counter-clockwise if PVP / clockwise if NXP) until you get to a button that is a primary color (R, G, B), then press that button.
- **PVS** or **NXS:** Start from the last colored button you pressed (or the NW button if you have not pressed any yet). Go (counter-clockwise if PVS / clockwise if NXS) until you get to a button that is a secondary color (C, M, Y), then press that button.
- **OPP:** Press the button that is diametrically opposite to the last button you pressed. If your last button pressed was **Outer Center** then press **Inner Center** and vice versa. Otherwise, if this is the first instruction, press **Outer Center.**

The following instructions will alter the next set of instructions. If you incorrectly handled another instruction after these instructions, undo the swaps until you come across the modifier instructions again. If you correctly handled an even number of the same instructions before (I.E INV and ERT), then undo the specified swaps for the rest of the instructions.

- **SWP:** Repeat the last colored button input or press the NW colored button otherwise. If an instruction requests **Outer Center,** press **Inner Center** instead and vice versa for the next set of instructions. Account for time specific instructions.
- **INV** or **ERT:** Press **Outer Center** if there was an odd number of previous presses, or **Inner Center** otherwise. All Red presses are swapped with Cyan presses; all Green presses are swapped with Magenta presses; and all Blue presses are swapped with Yellow presses. For example, if you have to press Red for one of the instructions, press Cyan instead and vice versa.

Instructions (Continued):

The following instructions CANNOT be skipped and are also instructions that show up last. DO NOT apply the swaps to these instructions. The number of solved/unsolved modules will take into account once you interact for these instructions.

- **FIN:** ONLY when the last seconds digit on the countdown timer is the least significant digit of the number of unsolved modules, if the number of solved modules is even, press **Inner Center**, otherwise press **Outer Center**.
- **ISH:** Count X buttons clockwise starting from the last colored button you pressed, or the NW button if you have not pressed a colored button yet, where X is the number of **Inner Center** and **Outer Center** buttons you pressed up to this point. Press that button when the last seconds digit on the countdown timer is the least significant digit of the number of unsolved modules on the bomb.
- **ALE:** ONLY when the last seconds digit on the countdown timer is the least significant digit of the number of solved modules, if there are an even number of pressed colored buttons (R, Y, G, C, B, M) press the button diametrically opposite to the last colored button you pressed, or the SE button if there were none; Otherwise, press the button whose color is a complementary of last colored button you pressed (R <-> C, G <-> M, B <-> Y).

Appendix: Base-24 Conversion

The table on the right shows a quick lookup for the base 24 values on the table, in base-10 (DEC). To convert a base-24 number into base-10 (DEC):

1. Start on the first base-24 digit with the current value of 0.
2. Add the base-24 value of the digit you are on.
3. If this is not the last base-24 digit, multiply the current value by 24 and go to the next digit.
4. Repeat steps 2 and 3 until you have went through all of the base-24 digits.
5. You should now have a number in base 10 or in decimal.

Base 24	DEC	Base 24	DEC
0 - 9	0 - 9	J	19
A	10	K	20
B	11	L	21
C	12	M	22
D	13	N	23
E	14	10	24
F	15	11	25
G	16	12	26
H	17	20	48
I	18	...	...

Appendix — HexDex

To convert a base-10 number to hexadecimal:

1. Divide the number by 16. Obtain the remainder and quotient.
2. Convert the remainder into a hexadecimal digit. See the corresponding table for a quick reference.
3. Repeat steps 1 and 2 with the quotient as the new number. Keep repeating until the quotient is zero.
4. Reverse the order of the hexadecimal digits obtained.
5. Remove leading zeros.

DEC	HEX
0 - 9	0 - 9
10	A
11	B
12	C
13	D
14	E
15	F
16	10
17	11
26	1A
...	...

Appendix — PR1M3

- A prime number is referred to a number that is only divisible by 1 and itself. 1 is not considered prime even though it is divisible by 1 and itself.
- Prime numbers (to 20): 2, 3, 5, 7, 11, 13, 17, 19