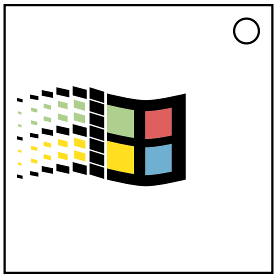
On the Subject of Michaelsoft Binbows



36.372896796384055, 139.05839087066113

This module features four colored intractable segments in a similar shape to the Microsoft logo.

After interacting with any of the four segments, there is a button that takes you back to the main appearance.

- The top-left segment (Green) will turn the module green and will display the encrypted email (12-letter word).
- The top-right segment (Red) will turn the module red and will display a five-digit hexadecimal number.
- The bottom-left segment (Yellow) will turn the module yellow and will display an initialization vector (one random letter).
- The bottom-right segment (Blue) will turn the module blue and will display a QWERTY keyobard (with special characters) for submission.

If the input is not the re-encrypted email, the module will strike.

Decryption (EBC)

Take the hexdecimal number obtained from the top-right segment and convert it to binary. After doing so, take the binary string and make five even rows of four binary bits. This is your key for the ciphers.

For each letter from the encrypted email, convert it to binary using the binary table below. Then, append each bit to the end of its row (first bit goes to the top row ... last bit goes to the bottom row).

For each row, if the number of 1s are odd in the row, the new bit will be 1. Otherwise, the new bit will be 0.

Convert the newly-obtained binary string into a letter using the binary table below. Continue this process with the remaining letters. You will obtain the decrypted twelve-letter word.

Encryption (CBC)

After obtaining the decrypted twelve-letter word, convert each letter to binary using the binary table below, and append each bit from the obtained string of binary digits to the end of its row.

For each row, if the number of 1s are odd in the row, the new bit will be 1. Otherwise, the new bit will be 0.

Take the initialization vector from the bottom-left segment and convert it to binary using the binary table below, and XOR the obtained binary string.

XOR returns true if exactly one input is true, otherwise it's false.

Convert this newly-obtained binary string to a letter using the binary table below, append to a string of letters.

This newly-obtained binary string will now be the new vector. Repeat this process until all letters have been encrypted.

Binary Table					
A	00000	L	01011	W	10110
B	00001	M	01100	X	10111
C	00010	N	01101	Y	11000
D	00011	O	01110	Z	11001
E	00100	P	01111	@	11010
F	00101	Q	10000	$	11011
G	00110	R	10001	%	11100
H	00111	S	10010	&	11101
I	01000	T	10011	?	11110
J	01001	U	10100	=	11111
K	01010	V	10101		

Michaelsoft's Activation Deal

1. Take first letter of the encrypted email and convert it to binary using the binary table above.
2. Take the initial vector from the bottom-left segment and convert it to binary using the binary table above.
3. XOR both binary numbers. The new binary number is the new vector. Convert the new binary number back to a letter.
4. Repeat with second letter and newly-obtained vector and so on.
5. Profit. 🤑

Thank you for partaking in the Michaelsoft Activation Deal!