

1. Run Round: This will run all subroutines (2, 5, 6, 7) in the correct order to simulate a normal round.
2. Add Round Key: This runs the subroutine dealing with round key (Also takes care of generating the expanded key).
3. Dropdown [1-32]: This simulates the round you’re currently on. This will need to be manually updated. This is primarily used for the round key subroutine [2].
4. Dropdown [128, 192, 256]: This is the key size you’d like to use.
5. Sub Bytes: This runs the subroutine dealing with sub bytes. Will use the SBox currently selected [14].
6. Shift Rows: This simulates the shift rows subroutine.
7. Mix columns: This simulates the mix columns subroutine.
8. Dropdown [OFB, CFB, CBC]: This changes the mode of operation to use whichever mode you choose here.
9. Top Left Text Field: This text field changes use depending on current mode [13]. Under 2 PTexts 1 Key, it will use this as a plain text. Under 1 PTexts 2 Keys, it will use this as a key. This primarily effects the first row images [19, 21, 23].
10. Top Right Text Field: This text field changes use depending on current mode [13]. Under 2 PTexts 1 Key, it will use this as the key. Under 1 PTexts 2 Keys, it will use this as a plain text to be acted on by the keys. This primarily effects all images [19, 20, 21, 22, 23, 24].
11. Bottom Left Text Field: This text field changes use depending on current mode [13]. Under 2 PTexts 1 Key, it will use this as a plain text. Under 1 PTexts 2 Keys, it will use this as a key. This primarily effects the first row images [20, 22, 24].
12. Bottom Right Text Field: This is the initialization vector, primarily effecting all images [19, 20, 21, 22, 23, 24].
13. # Ptext # Key: This will change the mode of the visualization to use either two plaintexts with one key, or two keys and one plaintext.
14. SBox Status: This button will allow you to use all 0’s for the SBox, or use the default SBox that is built in.
15. 🡨: Allows you to go back in your past for the center column.
16. 🡪: Allows you to go forward, assuming you’ve gone in the history, for the center column.
17. Blank button: Not used. This is used for spacing.
18. Visualization Dropdown: Greyscale and color scale are both ways to visualize the current values in the first 16 bytes. The other two, histogram and bit compare are ways to visualize the distribution. The distribution visualization shows the whole set of data, not just the first 16 bytes.
19. Top Left Image: Visually shows the initial plaintext and key, never changes unless certain values [9, 10] are touched.
20. Bottom Left Image: Visually shows the initial plaintext and key, never changes unless the certain values [10, 11] are touched.
21. Top Center Image: Visually shows the current state of the encryption, using certain values [9, 10].
22. Bottom Center Image: Visually shows the current state of the encryption, using certain valus [10, 11].
23. Top Right Image: Visually shows the result of a normal encryption using AES and the settings from above [4, 8] and certain values [9, 10].
24. Bottom Right Image: Visually shows the result of a normal encryption using AES and the settings from above [4, 8] and certain values [10, 11].
25. TODO: Show the entropy of the first encryption [23].
26. TODO: Show the entropy of the second encryption [24].