CS454 - HW2

I implemented AES by first Gathering the SBOX's and rcon in hex. Afterword I wrote each needed function to implement AES where I hit my first snag. How to convert an input of hex string like 0123456789abcdef into a 4x4 hex matrix. So I then wrote a separate function for it converting each segment of 8 characters into an integer and then appending it to a list.

To test that the 4x4 matrix was correct, a simple for loop prints out each row of the list.

I also had to then put the 4x4 matrix output back to string form to make them easily interpretable for debugging and for the output of the ciphertext. To fix this I then created a string and then a nested for loop that went through the passed argument of the 4x4 state list.

Question 1: Sub-Bytes
Implemented a nested for loop that iterated the state over the sbox.

Question 2: Shift rows
Took the state and transposed using a for loop and shifting each row by one additional position.

Question 3: Mix Columns
The next issue encountered was mix columns functions. Now this column was incompatible with the 4x4 matrix. To make it work I created a guml function to preform the multiplication in the Galios Field and then adjusted it to work with the new list.

Question 4: Add round key
in add round key the function apply's the round key to the state via a nested for loop.

Question 5: key Expansion
Made two sub functions: sub_word and rot_word.
sub word applies the sbox to a word and rot word applies an or rotation. The key expansion function goes through a for loop that expands the initial key and apply's the rcon list and subword and rot word to it.

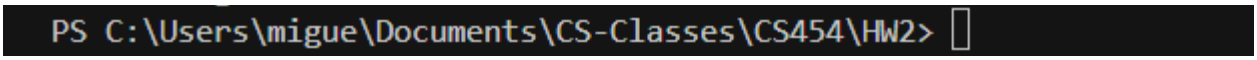
Qustion 6: Assembly

Since all AES steps are in functions ran each one in proper order so expanding the key, then equating the state to the initial round key then doing 9 rounds of encryption with sub_bytes, shift_rows, mix_columns, and add_round_key in that order. Then on the final round did the same thing except without mix_columns.

Question 7: Test and Verification
Added Print statements for every major AES function that both printed the string hex and 4x4

hex matrix version of the output.
Also added a bits changed function to track bits changed after each round.

```
PS C:\Users\migue\Documents\CS-Classes\CS454\HW2> python3 .\AES.py
Plaintext: 0123456789abcdeffedcba9876543210
Key: 0f1571c947d9e8590cb7add6af7f6798

Initial Round text: 0ecef2d936726b2b34251755aeb64e88

Round 1
Round text: 650fc04d74c7e8d070ffe82a753fca9c
Bits changed due to avalanche effect: 56

Round 2
Round text: 5c6b05f47b72a26db43431129a9b7f94
Bits changed due to avalanche effect: 66

Round 3
Round text: 71485c7d15dcdaa92674c7bd247e229c
Bits changed due to avalanche effect: 54

Round 4
Round text: f8b40c4c673724ffaea5c1eae82197bc
Bits changed due to avalanche effect: 66

Round 5
Round text: 72bacb041e06d4fab220bc65006de74e
Bits changed due to avalanche effect: 57

Round 6
Round text: 0a89c185d9f9c5e5d8f7f7fb567b1114
Bits changed due to avalanche effect: 53

Round 7
Round text: dba1f877186d8bbaa830084effd5d7aa
Bits changed due to avalanche effect: 64
Bits changed due to avalanche effect: 64

Round 8
Round text: f9e98f2b1b342f084fc98549bfbf8189
Bits changed due to avalanche effect: 68

Round 9
Round text: cc3eff3ba16759af048502aaa1005f34
Bits changed due to avalanche effect: 64

Final Round:

Ciphertext: ff0869640b53341484bfab8f4a7c43b9
Bits changed due to avalanche effect: 60
```



Question 8: Avalanche Effect

Normal Output:

```
PS C:\Users\migue\Documents\CS-Classes\CS454\HW2> python3 .\AES.py
Plaintext: 0123456789abcdeffedcba9876543210
Key: 0f1571c947d9e8590cb7add6af7f6798

Initial Round text: 0ecef2d936726b2b34251755aeb64e88

Round 1
Round text: 650fc04d74c7e8d070ffe82a753fca9c
Bits changed due to avalanche effect: 56

Round 2
Round text: 5c6b05f47b72a26db43431129a9b7f94
Bits changed due to avalanche effect: 66

Round 3
Round text: 71485c7d15dcdaa92674c7bd247e229c
Bits changed due to avalanche effect: 54

Round 4
Round text: f8b40c4c673724ffaea5c1eae82197bc
Bits changed due to avalanche effect: 66

Round 5
Round text: 72bacb041e06d4fab220bc65006de74e
Bits changed due to avalanche effect: 57

Round 6
Round text: 0a89c185d9f9c5e5d8f7f7fb567b1114
Bits changed due to avalanche effect: 53

Round 7
Round text: dba1f877186d8bbaa830084effd5d7aa
Bits changed due to avalanche effect: 64
Bits changed due to avalanche effect: 64

Round 8
Round text: f9e98f2b1b342f084fc98549bfbf8189
Bits changed due to avalanche effect: 68

Round 9
Round text: cc3eff3ba16759af048502aaa1005f34
Bits changed due to avalanche effect: 64

Final Round:

Ciphertext: ff0869640b53341484bfab8f4a7c43b9
Bits changed due to avalanche effect: 60
```

```
PS C:\Users\migue\Documents\CS-Classes\CS454\HW2>
```

1 character changed in the Plaintext:

```
PS C:\Users\migue\Documents\CS-Classes\CS454\HW2> python3 .\AES.py
Plaintext: 9123456789abcdeffedcba9876543210
Key: 0f1571c947d9e8590cb7add6af7f6798

Initial Round text: 9ecef2d936726b2b34251755aeb64e88

Round 1
Round text: 3e0fc04dd4c7e8d0d0ffe82a8e3fca9c
Bits changed due to avalanche effect: 56

Round 2
Round text: b9ef248184f6c1c24ba373c880885e4e
Bits changed due to avalanche effect: 61

Round 3
Round text: 0a81231ad8ee275abf4b94d1500c5931
Bits changed due to avalanche effect: 64

Round 4
Round text: 7f9f91c7caed85e93c473225c7d6abf2
Bits changed due to avalanche effect: 58

Round 5
Round text: b20b29850987a1f7775bc809f93477fc
Bits changed due to avalanche effect: 59

Round 6
Round text: 7e1487354dfc8c8e6cdffb491fd80b84
Bits changed due to avalanche effect: 63

Round 7
Round text: 51030c4bd2826ca42f54058e472617c0
Bits changed due to avalanche effect: 62

Round 8
Round text: 154c1555d64b67ec844035465f48c298
Bits changed due to avalanche effect: 67

Round 9
Round text: 515d3337ce0fb85e55b29536893db0fc
Bits changed due to avalanche effect: 71

Final Round:

Ciphertext: 65f6bc1cf8f415add916a52fe2e90791
Bits changed due to avalanche effect: 65
```

Decrypt AES:

```
PS C:\Users\migue\Documents\CS-Classes\CS454\HW2> python3 .\AES.py
Plaintext: 0123456789abcdeffedcba9876543210
Key: 0f1571c947d9e8590cb7add6af7f6798

Encrypting with AES

Initial Round text: 0ecef2d936726b2b34251755aeb64e88

Round 1
Round text: 650fc04d74c7e8d070ffe82a753fca9c
Bits changed due to avalanche effect: 56

Round 2
Round text: 5c6b05f47b72a26db43431129a9b7f94
Bits changed due to avalanche effect: 66

Round 3
Round text: 71485c7d15dcdaa92674c7bd247e229c
Bits changed due to avalanche effect: 54

Round 4
Round text: f8b40c4c673724ffaea5c1eae82197bc
Bits changed due to avalanche effect: 66

Round 5
Round text: 72bacb041e06d4fab220bc65006de74e
Bits changed due to avalanche effect: 57

Round 6
Round text: 0a89c185d9f9c5e5d8f7f7fb567b1114
Bits changed due to avalanche effect: 53

Round 7
Round text: dba1f877186d8bbaa830084effd5d7aa
Bits changed due to avalanche effect: 64

Round 8
Round text: f9e98f2b1b342f084fc98549bfbf8189
Bits changed due to avalanche effect: 68

Round 9
Round text: cc3eff3ba16759af048502aaa1005f34
Bits changed due to avalanche effect: 64

Final Round:

Ciphertext: ff0869640b53341484bfab8f4a7c43b9
```

```
Bits changed due to avalanche effect: 60

Decrypting with AES

Plaintext: c54b471c6d85d3506629ddcc8780800f
```