Aubrey gatewood 2/13/2024

Encrypt function:

I first open the key file to generate the round keys. Then I make a bitvector out of it and generate the key schedule. Then I made a bitvector from the plaintext file.

My while loop is true while there are more bits to read in the plaintext file. Then I initialize the state vector and do the initial xor with round-keys[0] element.

Then I start iterating over the 14 rounds. I ran subbytes, did the row shifts, then I had to convert back to a bitvector because I used numpy to do the array shifts. That was a mistake because it kept me from being able to change the steps for decrypt. After that, I do the matrix multiplication to get the MixColumns operation done. After that I xor with the round key, permute statearray to be prepared for the next round, and then I add the hex string of the bitvector to an output variable called tempstring. At the end of the 14 rounds I output tempstring to the ciphertext file and this is my output:

```
3ba1ab4b7fe412ca26c7a25cff913d1b748da805c97c83554d9e9cf5b12243ff03a8c6b6dcbc52075
0a14df9b646fa480d1e64cc2e9174a23dbed6aad77144350ff768093cf7571852a26ffa36fe47652a54
6acf9d4bc1ad395a92553b4b7e0a5a7811d7b95d95cacc117e344ac093da247168cd4bbbda5bc28
66fd044c8ca18ecd2b6a78bfe19520f22b7fa12862132e32ee78c5e4200166c40f1a93f9b08c5f67b9
bde38d34ed34bd03183a529a5a62d81b1cf084832fcb9139a51100a04c7c631d3fbfa5bb9b8cbe97
0f02213ab07d3e179313142865fb8b022241552567964250cfa2aa97c59223d30a2a7da8974d0f6c3
4f4f46ed6cab53e483f95d4ed157bb78ce078a88397c9d656830fadd080d729ac7428a6ca3c17ad67
d0cf16d35a8ecb35cd818a380309332c4cc29d00b6fe542b67724295b49804b2122b5b24e6f09e22
451bb77c6876d51b7294b405dcff0cdc83754538442fcc766bfe4fac839e932f757aebbe7f43c87d08
249c6ef50d9adefa8eca175785ba0dbc31e2e61ba32a75f596894ea736bcea8f351d3c4574539e7ad
760c4a0c4b252e2dbc859c4b0a6b44fbf29b3fa7fddeace3855c675130ef65d4fa7f8125d4575f329c
c93d75d14fdcb1419678cae4d686d4b72f56ac4d7974e3b1f1bbb3776dda5db94b7d2ef1f73f96f7b
24378a1e299271006cd478bd84fe7a24c67794e663668c918bdb65097099351e1ebf6e7d1148754f
1051d33156e4fb7e96cce8f976f6a0ad71d12b10d1b43458c02002bf1fc14c9c63e9033dfdcbc9baa
e76efc8e12a850fdd21ead4e9b14fb359a27fc4943b0d76714
```

Decrypted I could not get to work because I did a bad job managing my data types doing encrypt, so when I went to do decrypt, moving the steps around caused an unholy number of type errors