> CSE350/550: Network Security - Programming Assignment no. 2
> (c) Ankit Kumar (2021015) & Lakshay Chauhan (2021060)

We were required to develop a program to encrypt (and similarly decrypt) a 128-bit plaintext using AES that uses keys of size 128 bit, and 10 rounds.

The whole code is divided into various functions involving helper functions, aes helper functions, encryption and decryption functions.

1. Initialization and S-Boxes:

The constructor initializes the AES object with a 128-bit key (16 characters) and loads the substitution boxes (S-box for encryption and inverse S-box for decryption) from external files. These S-boxes are used for the byte substitution step.

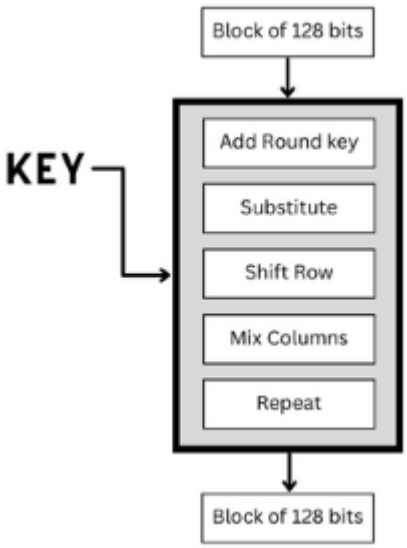
2. Utility Functions:

- `printHex` displays blocks of data in hexadecimal format.
- `multiplyWithinGaloisField` performs `multiplication` in the Galois field,essential for the mix columns step.
- `arrayToMatrix` and `matrixToArray` convert between linear arrays and 4x4 matrices, facilitating operations that work with AES state matrices.

3. Key Expansion:

- Before the actual encryption process begins, the input key undergoes an expansion using the `keyExpansion` method. This process generates a series of round keys from the initial key. Each round key is derived from the previous one through a combination of byte substitution (using the S-box), byte rotation, and XOR operations with a round constant.

4. Encrption:



1. Initial Round
    - `AddRoundKey`: The first operation of the encryption process is to XOR the plaintext block with the initial round key (derived from the key expansion process).
2. Main Rounds (1 to 9): Each of these rounds includes the following four steps
    - `SubBytes`: A non-linear substitution step where each byte is replaced with another according to the S-box.
    - `ShiftRows`: A transposition step where each row of the state is shifted cyclically a certain number of steps.
    - `MixColumns`: A mixing operation which operates on the columns of the state, combining the four bytes in each column.
    - `AddRoundKey`: Each byte of the state is XORed with the round key.
      The `mixColumns` step is not performed in the final (10th) round.
3. Final Round (10th Round):
    - The final round includes the `SubBytes`, `ShiftRows`, and `AddRoundKey` steps, but omits the `MixColumns` step.

5. AES Decryption Steps:

-Decryption follows the reverse order of encryption, applying the inverse of each operation. It's worth noting that the round keys are applied in reverse order during decryption.

1. Key Expansion:
    - Similar to encryption, the decryption process begins with key expansion. The same key expansion function is used, but the round keys are used in reverse order.
2. Initial Round:
    - AddRoundKey: The ciphertext is XORed with the last round key from the expanded key set.
3. Main Rounds (1 to 9): Each of these rounds consists of the following steps, applied in reverse order compared to encryption:
    - `InvShiftRows`: The inverse of the `ShiftRows` step, rows are cyclically shifted in the opposite direction.
    - `InvSubBytes`: The inverse of the `SubBytes` step, where bytes are substituted back using the inverse S-box.
    - `AddRoundKey`: The round key is XORed with the state.
    - `InvMixColumns`: The inverse of the MixColumns step, unmixing the columns of the state.
      The `InvMixColumns` step is performed after the `AddRoundKey` step, which is a reversal from the encryption process and is not applied in the final (10th) round.
4. Final Round (10th Round):
    - The final round includes `InvShiftRows`, `InvSubBytes`, and `AddRoundKey`, omitting the `InvMixColumns` step.

6. Testing and Verification:

The program includes facilities to debug and print intermediate states in hexadecimal format, aiding in the verification of: - The correctness of the encryption by decrypting the ciphertext and comparing it to the original plaintext. - The equivalence of the output of the 1st encryption round with the output of the 9th decryption round, and vice versa for the 9th encryption round and the 1st decryption round.

7. Testcases

- **Testcase 1**:
  - **Plaintext**: nosferatuoforava
  - **Key**: heyyoutherecanwe
  - **Ciphertext**: 3341b00b438214de68e7dc36522a4c64
  - Encryption:

```
PS E:\Github\Network Security\senet\aes> python .\aes.py encrypt "nosferatuoforava" "heyyoutherecanwe"
plain text: nosferatuoforava
ROUND 0         0x06 0x0a 0x0a 0x1f 0x0a 0x07 0x15 0x1c 0x10 0x1d 0x03 0x0c 0x13 0x0f 0x01 0x04
ROUND 1         0xf5 0x11 0x65 0x66 0x1c 0x95 0x20 0x14 0x12 0x84 0xe8 0xea 0x69 0x5f 0xe3 0xa6
ROUND 2         0x7b 0xb0 0xf8 0x00 0x14 0x57 0x81 0xa1 0x7c 0x83 0x99 0x86 0xd1 0xb8 0xde 0x63
ROUND 3         0x7c 0xf9 0x33 0xd9 0x8c 0xb4 0x24 0xf6 0xdd 0x12 0x15 0x06 0xa9 0x8b 0xf2 0x0d
ROUND 4         0xe8 0x87 0xa4 0xca 0xcc 0x3b 0xbf 0xc9 0x9d 0xef 0x5e 0x12 0x39 0xb7 0x91 0x03
ROUND 5         0x55 0x12 0x31 0x5d 0x87 0xa4 0x20 0x83 0x94 0xff 0xd1 0x7b 0xed 0x7b 0x9b 0x64
ROUND 6         0x93 0x21 0x65 0x8e 0x04 0xa3 0xa5 0x2b 0x18 0xd8 0x29 0x13 0x59 0xaf 0xd4 0x57
ROUND 7         0xb5 0x71 0x21 0x39 0xb3 0x0f 0x3b 0xc1 0xdc 0x81 0xc5 0xa6 0x65 0x35 0x60 0x54
ROUND 8         0x9e 0x3f 0xa2 0xd8 0x81 0x25 0xc9 0xb4 0x14 0x04 0xdf 0x76 0x0a 0xb0 0x26 0xb1
ROUND 9         0x7f 0xf2 0xce 0xd9 0x70 0x4f 0x13 0xc6 0xbe 0xe2 0xf8 0xa0 0xc8 0x7e 0x9d 0x77
ROUND 10        0x33 0x41 0xb0 0x0b 0x43 0x82 0x14 0xde 0x68 0xe7 0xdc 0x36 0x52 0x2a 0x4c 0x64
cipher text: 3341b00b438214de68e7dc36522a4c64
```

  - Decryption:

```
PS E:\Github\Network Security\senet\aes> python .\aes.py decrypt 3341b00b438214de68e7dc36522a4c64 heyyoutherecanwe
cipher text: 3341b00b438214de68e7dc36522a4c64
ROUND 0         0x33 0x41 0xb0 0x0b 0x43 0x82 0x14 0xde 0x68 0xe7 0xdc 0x36 0x52 0x2a 0x4c 0x64
ROUND 1         0x7f 0xf2 0xce 0xd9 0x70 0x4f 0x13 0xc6 0xbe 0xe2 0xf8 0xa0 0xc8 0x7e 0x9d 0x77
ROUND 2         0x9e 0x3f 0xa2 0xd8 0x81 0x25 0xc9 0xb4 0x14 0x04 0xdf 0x76 0x0a 0xb0 0x26 0xb1
ROUND 3         0xb5 0x71 0x21 0x39 0xb3 0x0f 0x3b 0xc1 0xdc 0x81 0xc5 0xa6 0x65 0x35 0x60 0x54
ROUND 4         0x93 0x21 0x65 0x8e 0x04 0xa3 0xa5 0x2b 0x18 0xd8 0x29 0x13 0x59 0xaf 0xd4 0x57
ROUND 5         0x55 0x12 0x31 0x5d 0x87 0xa4 0x20 0x83 0x94 0xff 0xd1 0x7b 0xed 0x7b 0x9b 0x64
ROUND 6         0xe8 0x87 0xa4 0xca 0xcc 0x3b 0xbf 0xc9 0x9d 0xef 0x5e 0x12 0x39 0xb7 0x91 0x03
ROUND 7         0x7c 0xf9 0x33 0xd9 0x8c 0xb4 0x24 0xf6 0xdd 0x12 0x15 0x06 0xa9 0x8b 0xf2 0x0d
ROUND 8         0x7b 0xb0 0xf8 0x00 0x14 0x57 0x81 0xa1 0x7c 0x83 0x99 0x86 0xd1 0xb8 0xde 0x63
ROUND 9         0xf5 0x11 0x65 0x66 0x1c 0x95 0x20 0x14 0x12 0x84 0xe8 0xea 0x69 0x5f 0xe3 0xa6
ROUND 10        0x06 0x0a 0x0a 0x1f 0x0a 0x07 0x15 0x1c 0x10 0x1d 0x03 0x0c 0x13 0x0f 0x01 0x04
plain text: nosferatuoforava
```

- **Testcase 2**:
  - **Plaintext**: ankitkumarkitkat
  - **Key**: onepiece is real
  - **Ciphertext**: 841ce41c7dfee8128986c2d554993453
  - Encryption:

```
PS E:\Github\Network Security\senet\aes> python .\aes.py encrypt ankitkumarkitkat "onepiece is real"
plain text: ankitkumarkitkat
ROUND 0         0x0e 0x00 0x0e 0x19 0x1d 0x0e 0x16 0x08 0x41 0x1b 0x18 0x49 0x06 0x0e 0x00 0x18
ROUND 1         0x88 0x26 0x98 0x91 0x44 0x74 0xfc 0xdd 0x0a 0x95 0x10 0x8b 0x1f 0xb3 0x8b 0xfa
ROUND 2         0x63 0x09 0x4f 0xc8 0x04 0xf7 0x64 0xeb 0x64 0x45 0x4c 0xa6 0x96 0xd8 0xdd 0xc2
ROUND 3         0x48 0x19 0x06 0x93 0x85 0x8c 0x39 0x2f 0x33 0x1e 0x9c 0x12 0xa6 0x89 0x20 0xfe
ROUND 4         0x59 0x0d 0x20 0x36 0x1d 0x2a 0x97 0x95 0xbb 0x94 0x70 0x16 0xa3 0x34 0x3a 0xd6
ROUND 5         0x70 0xae 0x0c 0x49 0x0b 0x88 0x6b 0x42 0x6f 0x62 0xf5 0x69 0xfb 0x77 0xbd 0x8d
ROUND 7         0xb1 0x66 0x58 0x34 0x8c 0x4e 0x76 0x24 0x6d 0x5b 0x12 0x5d 0x95 0x8e 0x78 0xc2
ROUND 8         0x95 0x8e 0x31 0xde 0xa2 0x77 0x1b 0x7f 0x92 0xd6 0xc3 0xa0 0xac 0xcf 0x4a 0x03
ROUND 9         0x8a 0xc7 0x16 0x57 0xb4 0x02 0x49 0x36 0x99 0x23 0x40 0xba 0x13 0xcd 0x7c 0xb2
ROUND 10        0x84 0x1c 0xe4 0x1c 0x7d 0xfe 0xe8 0x12 0x89 0x86 0xc2 0xd5 0x54 0x99 0x34 0x53
cipher text: 841ce41c7dfee8128986c2d554993453
```

  - Decryption:

```
PS E:\Github\Network Security\senet\aes> python .\aes.py decrypt 841ce41c7dfee8128986c2d554993453 "onepiece is real"
cipher text: 841ce41c7dfee8128986c2d554993453
ROUND 0         0x84 0x1c 0xe4 0x1c 0x7d 0xfe 0xe8 0x12 0x89 0x86 0xc2 0xd5 0x54 0x99 0x34 0x53
ROUND 1         0x8a 0xc7 0x16 0x57 0xb4 0x02 0x49 0x36 0x99 0x23 0x40 0xba 0x13 0xcd 0x7c 0xb2
ROUND 2         0x95 0x8e 0x31 0xde 0xa2 0x77 0x1b 0x7f 0x92 0xd6 0xc3 0xa0 0xac 0xcf 0x4a 0x03
ROUND 3         0xb1 0x66 0x58 0x34 0x8c 0x4e 0x76 0x24 0x6d 0x5b 0x12 0x5d 0x95 0x8e 0x78 0xc2
ROUND 4         0xfe 0x25 0x08 0x0b 0xf9 0xac 0x6c 0xa6 0x83 0x41 0x96 0x7a 0xf3 0x85 0xff 0xeb
ROUND 5         0x70 0xae 0x0c 0x49 0x0b 0x88 0x6b 0x42 0x6f 0x62 0xf5 0x69 0xfb 0x77 0xbd 0x8d
ROUND 7         0x48 0x19 0x06 0x93 0x85 0x8c 0x39 0x2f 0x33 0x1e 0x9c 0x12 0xa6 0x89 0x20 0xfe
ROUND 8         0x63 0x09 0x4f 0xc8 0x04 0xf7 0x64 0xeb 0x64 0x45 0x4c 0xa6 0x96 0xd8 0xdd 0xc2
ROUND 9         0x88 0x26 0x98 0x91 0x44 0x74 0xfc 0xdd 0x0a 0x95 0x10 0x8b 0x1f 0xb3 0x8b 0xfa
ROUND 10        0x0e 0x00 0x0e 0x19 0x1d 0x0e 0x16 0x08 0x41 0x1b 0x18 0x49 0x06 0x0e 0x00 0x18
plain text: ankitkumarkitkat
```

- **Testcase 3**:
  - **Plaintext**: bijendranathjain
  - **Key**: pretty cool prof
  - **Ciphertext**: 4593374e10f0f25b80acc630f4675c63

- Encryption:

```
PS E:\Github\Network Security\senet\aes> python .\aes.py encrypt bijendranathjain "pretty cool prof"
plain text: bijendranathjain
ROUND 0         0x12 0x1b 0x0f 0x11 0x1a 0x1d 0x52 0x02 0x01 0x0e 0x18 0x48 0x1a 0x13 0x06 0x08
ROUND 1         0xd2 0x9c 0x2a 0x0c 0x11 0x7f 0x3c 0x60 0x54 0xa7 0x6e 0x07 0xbd 0x0b 0x8e 0xf6
ROUND 2         0x5c 0xb5 0xb1 0x96 0xc4 0x0b 0xb6 0xe2 0xfa 0xba 0xe8 0xae 0x0b 0xa8 0x11 0x91
ROUND 3         0xfa 0x1d 0x0b 0x2e 0xfc 0x30 0xc0 0xed 0x74 0x93 0x12 0x69 0x13 0xc0 0xbc 0xb1
ROUND 4         0x06 0x85 0x63 0x55 0xd0 0x77 0xe9 0xf0 0x37 0xd5 0x58 0x49 0x66 0x6e 0x96 0x2b
ROUND 5         0x50 0xfd 0xff 0x87 0x18 0xf7 0xf2 0x50 0xd0 0xf3 0x1b 0xbd 0xfb 0xa5 0x99 0x9e
ROUND 7         0x18 0x47 0x19 0xde 0xef 0x0e 0x98 0x17 0x73 0xa9 0x10 0xa1 0xba 0xab 0x9e 0xbd
ROUND 8         0x88 0xe5 0x50 0xb5 0x9b 0x96 0x1b 0xf4 0x7e 0xe3 0x7a 0x26 0x46 0x1c 0x9c 0xf0
ROUND 9         0x59 0xf5 0xbe 0x52 0x61 0x9d 0x2a 0x62 0x26 0xa2 0xd0 0x65 0x2e 0x9d 0x15 0xd9
ROUND 10        0x45 0x93 0x37 0x4e 0x10 0xf0 0xf2 0x5b 0x80 0xac 0xc6 0x30 0xf4 0x67 0x5c 0x63
cipher text: 4593374e10f0f25b80acc630f4675c63
```

- Decryption:

```
PS E:\Github\Network Security\senet\aes> python .\aes.py decrypt 4593374e10f0f25b80acc630f4675c63 "pretty cool prof"
cipher text: 4593374e10f0f25b80acc630f4675c63
ROUND 0         0x45 0x93 0x37 0x4e 0x10 0xf0 0xf2 0x5b 0x80 0xac 0xc6 0x30 0xf4 0x67 0x5c 0x63
ROUND 1         0x59 0xf5 0xbe 0x52 0x61 0x9d 0x2a 0x62 0x26 0xa2 0xd0 0x65 0x2e 0x9d 0x15 0xd9
ROUND 2         0x88 0xe5 0x50 0xb5 0x9b 0x96 0x1b 0xf4 0x7e 0xe3 0x7a 0x26 0x46 0x1c 0x9c 0xf0
ROUND 3         0x18 0x47 0x19 0xde 0xef 0x0e 0x98 0x17 0x73 0xa9 0x10 0xa1 0xba 0xab 0x9e 0xbd
ROUND 4         0x7f 0x67 0xc2 0xd6 0xfb 0x5a 0x5a 0x63 0xc9 0x10 0xd7 0x0b 0x6d 0xe2 0xe8 0x21
ROUND 5         0x50 0xfd 0xff 0x87 0x18 0xf7 0xf2 0x50 0xd0 0xf3 0x1b 0xbd 0xfb 0xa5 0x99 0x9e
ROUND 7         0xfa 0x1d 0x0b 0x2e 0xfc 0x30 0xc0 0xed 0x74 0x93 0x12 0x69 0x13 0xc0 0xbc 0xb1
ROUND 8         0x5c 0xb5 0xb1 0x96 0xc4 0x0b 0xb6 0xe2 0xfa 0xba 0xe8 0xae 0x0b 0xa8 0x11 0x91
ROUND 9         0xd2 0x9c 0x2a 0x0c 0x11 0x7f 0x3c 0x60 0x54 0xa7 0x6e 0x07 0xbd 0x0b 0x8e 0xf6
ROUND 10        0x12 0x1b 0x0f 0x11 0x1a 0x1d 0x52 0x02 0x01 0x0e 0x18 0x48 0x1a 0x13 0x06 0x08
plain text: bijendranathjain
```

- **Testcase 4**:
  - **Plaintext**: network security
  - **Key**: winter2024course
  - **Ciphertext**: 2e9a6bf909a7198ded59af9c1fa5946e
    - Encryption:

```
PS E:\Github\Network Security\senet\aes> python .\aes.py encrypt "network security" winter2024course
plain text: network security
ROUND 0         0x19 0x0c 0x1a 0x03 0x0a 0x00 0x59 0x10 0x41 0x51 0x00 0x1a 0x07 0x1b 0x07 0x1c
ROUND 1         0xdf 0xcd 0xed 0xad 0x4b 0x65 0xbb 0x92 0xfe 0x51 0x44 0xaa 0xf5 0x14 0x4a 0xed
ROUND 2         0x3f 0xe6 0x5f 0x56 0x84 0xf0 0x25 0x32 0xd1 0x4a 0x1c 0x9b 0xea 0x72 0x5c 0x8a
ROUND 3         0x12 0xe1 0x64 0x3c 0x63 0xdf 0xbd 0x81 0xa4 0x21 0xd0 0x72 0xe4 0x5f 0x22 0x5d
ROUND 4         0xef 0x9d 0xee 0x94 0x2d 0xa8 0xf8 0x92 0xc7 0x04 0xbf 0x91 0xf8 0xc7 0x67 0x31
ROUND 5         0xf9 0x15 0x16 0xfc 0x6b 0xec 0xf1 0xbe 0x9b 0x1a 0x86 0x01 0x99 0x48 0xc0 0x6d
ROUND 7         0xcc 0xb7 0x9e 0xcb 0x77 0x15 0x36 0x5a 0x1d 0xd4 0xe4 0x86 0xb6 0xa2 0x97 0x20
ROUND 8         0x5f 0x7d 0x54 0x97 0x3f 0xd5 0x17 0xd4 0x82 0xd6 0x27 0xbb 0x53 0xba 0x44 0x65
ROUND 9         0xa4 0x0e 0x12 0x8f 0x5c 0xce 0x3c 0xc7 0x47 0x84 0x03 0xd5 0xa1 0x53 0xd5 0xdb
ROUND 10        0x2e 0x9a 0x6b 0xf9 0x09 0xa7 0x19 0x8d 0xed 0x59 0xaf 0x9c 0x1f 0xa5 0x94 0x6e
cipher text: 2e9a6bf909a7198ded59af9c1fa5946e
```

    - Decryption:

```
PS E:\Github\Network Security\senet\aes> python .\aes.py decrypt 2e9a6bf909a7198ded59af9c1fa5946e winter2024course
cipher text: 2e9a6bf909a7198ded59af9c1fa5946e
ROUND 0         0x2e 0x9a 0x6b 0xf9 0x09 0xa7 0x19 0x8d 0xed 0x59 0xaf 0x9c 0x1f 0xa5 0x94 0x6e
ROUND 1         0xa4 0x0e 0x12 0x8f 0x5c 0xce 0x3c 0xc7 0x47 0x84 0x03 0xd5 0xa1 0x53 0xd5 0xdb
ROUND 2         0x5f 0x7d 0x54 0x97 0x3f 0xd5 0x17 0xd4 0x82 0xd6 0x27 0xbb 0x53 0xba 0x44 0x65
ROUND 3         0xcc 0xb7 0x9e 0xcb 0x77 0x15 0x36 0x5a 0x1d 0xd4 0xe4 0x86 0xb6 0xa2 0x97 0x20
ROUND 4         0x9e 0xc2 0x10 0x89 0xe5 0x14 0x5e 0xd7 0xe1 0xfa 0x01 0x7b 0x1e 0x02 0x8f 0x94
ROUND 5         0xf9 0x15 0x16 0xfc 0x6b 0xec 0xf1 0xbe 0x9b 0x1a 0x86 0x01 0x99 0x48 0xc0 0x6d
ROUND 7         0x12 0xe1 0x64 0x3c 0x63 0xdf 0xbd 0x81 0xa4 0x21 0xd0 0x72 0xe4 0x5f 0x22 0x5d
ROUND 8         0x3f 0xe6 0x5f 0x56 0x84 0xf0 0x25 0x32 0xd1 0x4a 0x1c 0x9b 0xea 0x72 0x5c 0x8a
ROUND 9         0xdf 0xcd 0xed 0xad 0x4b 0x65 0xbb 0x92 0xfe 0x51 0x44 0xaa 0xf5 0x14 0x4a 0xed
ROUND 10        0x19 0x0c 0x1a 0x03 0x0a 0x00 0x59 0x10 0x41 0x51 0x00 0x1a 0x07 0x1b 0x07 0x1c
plain text: network security
```