

I was programming this algorithm using python 3.9.1, the algorithm is Advanced Encryption Standard (AES)

Let's start discussing function this algorithm:

All incoming function don't return but using in the inverse, shift rows and inverse them, add rounds, mixing columns and inverse them, and take the text and make them a matrix, and take matrix to binary.

```
subBytes(sub)
inverseSubBytes(sub)
shiftRows(sub)
inverseShiftRows(sub)
add_round_key(sub, key)
mixingOneColumn(sub)
mixingColumns(sub)
inverseMixingColumns(sub)
bytesToMatrix(text)
matrixToBytes(matrix)
xor(a, b)
```

```
class AES(object):
    have function and return values
    __init__(self, master_key)
    _expand_key(self, master_key)
    encrypt_block(self, plaintext)
    function takes the plaintext and convert it
    decrypt_block(self, ciphertext)
    function takes the ciphertext and convert it
```

snpshots of output

```
... 0123456789ABCDEF0123456789ABCDEF
    0123456789ABCDEF0123456789ABCDEF
    encryption : a1ee5608b33af05470858608d1de080f
    Decreption : 0123456789abcdef0123456789abcdef
```