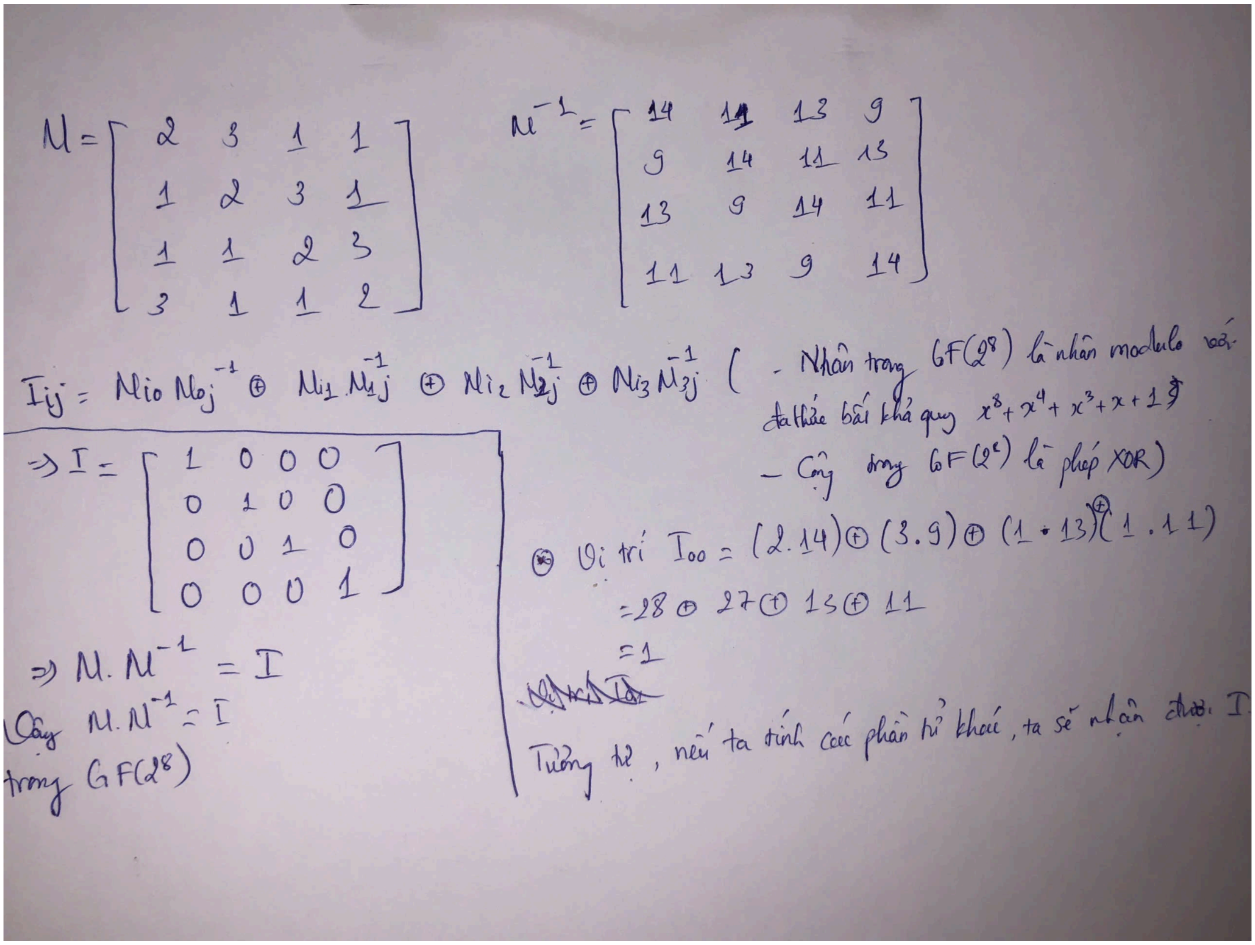
Week 5 task

Tên: Trần Hữu Đức
MSSV: 23520321

Task 1: Chứng minh M.M(^-1) = I trong GF(2^8) (mod $x^8 + x^4 + x^3 + x + 1$)



$$M = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \qquad M^{-1} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix}$$

$I_{ij} = M_{i0} M_{0j}^{-1} \oplus M_{i1} M_{1j}^{-1} \oplus M_{i2} M_{2j}^{-1} \oplus M_{i3} M_{3j}^{-1}$ (- Nhân trong GF(2^8) là nhân modulo với đa thức bất khả quy $x^8 + x^4 + x^3 + x + 1$ }
- Cộng trong GF(2^8) là phép XOR)

$$\Rightarrow I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$\Rightarrow M.M^{-1} = I$

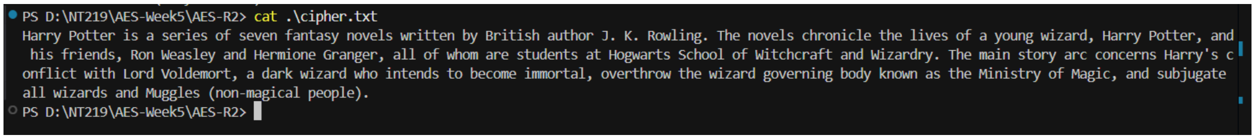
Vậy $M.M^{-1} = I$ trong GF(2^8)

⊛ Vị trí $I_{00} = (2.14) \oplus (3.9) \oplus (1.13) \oplus (1.11)$
$= 28 \oplus 27 \oplus 13 \oplus 11$
$= 1$

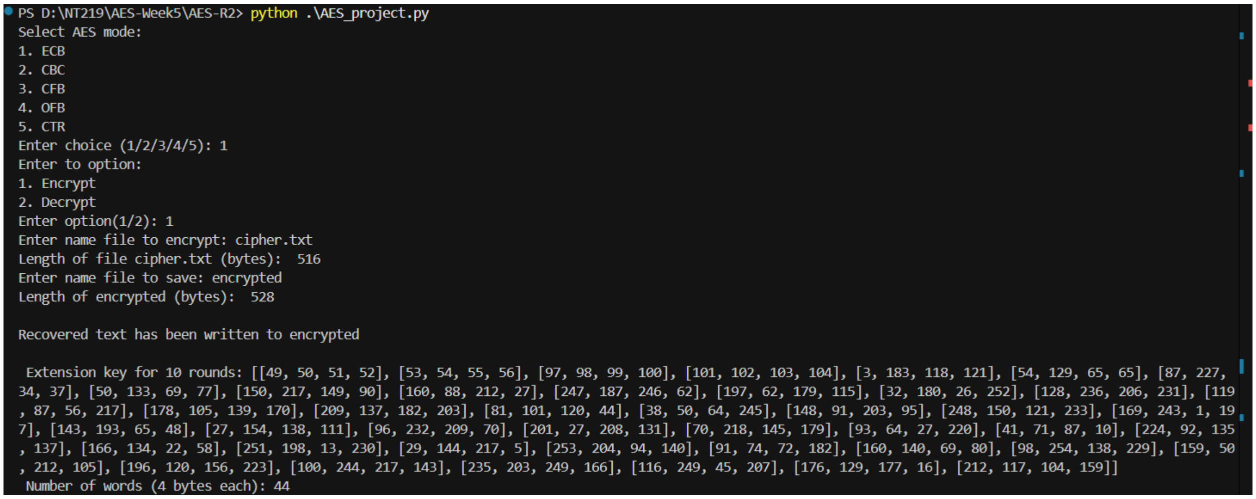
Tương tự, nếu ta tính các phần tử khác, ta sẽ nhận được I

Task 2: Sửa AES code để có thể mã hóa files (nhân đầu vào là file và lưu kết quả ra file)

plain text:

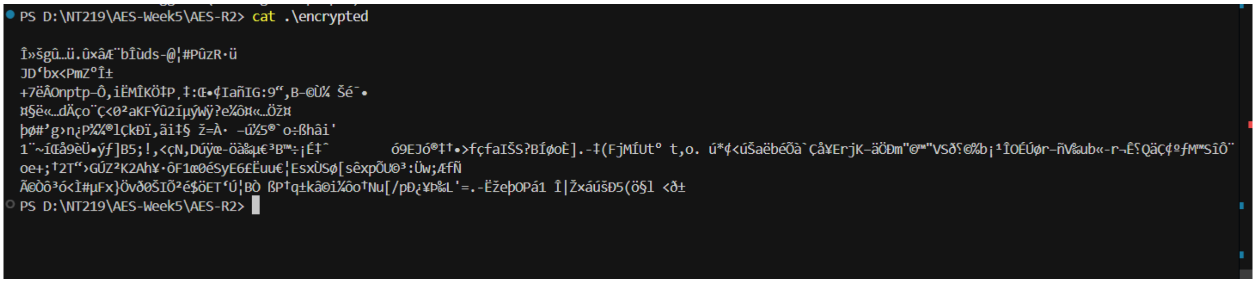


```
PS D:\NT219\AES-Week5\AES-R2> cat .\cipher.txt
Harry Potter is a series of seven fantasy novels written by British author J. K. Rowling. The novels chronicle the lives of a young wizard, Harry Potter, and
 his friends, Ron Weasley and Hermione Granger, all of whom are students at Hogwarts School of Witchcraft and Wizardry. The main story arc concerns Harry's c
onflict with Lord Voldemort, a dark wizard who intends to become immortal, overthrow the wizard governing body known as the Ministry of Magic, and subjugate
all wizards and Muggles (non-magical people).
PS D:\NT219\AES-Week5\AES-R2> 
```

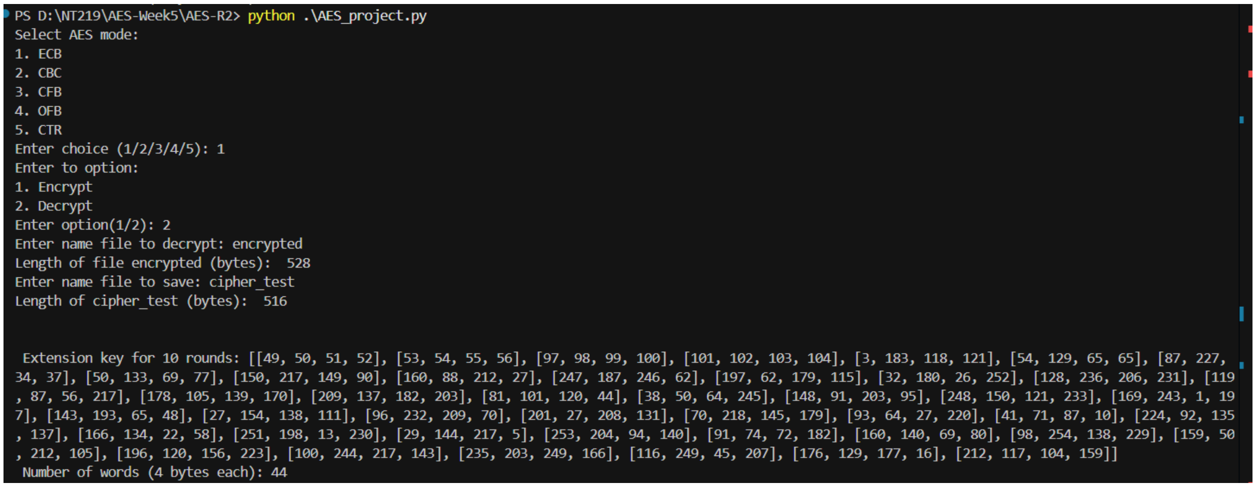


```
PS D:\NT219\AES-Week5\AES-R2> python .\AES_project.py
Select AES mode:
1. ECB
2. CBC
3. CFB
4. OFB
5. CTR
Enter choice (1/2/3/4/5): 1
Enter to option:
1. Encrypt
2. Decrypt
Enter option(1/2): 1
Enter name file to encrypt: cipher.txt
Length of file cipher.txt (bytes):  516
Enter name file to save: encrypted
Length of encrypted (bytes):  528

Recovered text has been written to encrypted

 Extension key for 10 rounds: [[49, 50, 51, 52], [53, 54, 55, 56], [97, 98, 99, 100], [101, 102, 103, 104], [3, 183, 118, 121], [54, 129, 65, 65], [87, 227,
34, 37], [50, 133, 69, 77], [150, 217, 149, 90], [160, 88, 212, 27], [247, 187, 246, 62], [197, 62, 179, 115], [32, 180, 26, 252], [128, 236, 206, 231], [119
, 87, 56, 217], [178, 105, 139, 170], [209, 137, 182, 203], [81, 101, 120, 44], [38, 50, 64, 245], [148, 91, 203, 95], [248, 150, 121, 233], [169, 243, 1, 19
7], [143, 193, 65, 48], [27, 154, 138, 111], [96, 232, 209, 70], [201, 27, 208, 131], [70, 218, 145, 179], [93, 64, 27, 220], [41, 71, 87, 10], [224, 92, 135
, 137], [166, 134, 22, 58], [251, 198, 13, 230], [29, 144, 217, 5], [253, 204, 94, 140], [91, 74, 72, 182], [160, 140, 69, 80], [98, 254, 138, 229], [159, 50
, 212, 105], [196, 120, 156, 223], [100, 244, 217, 143], [235, 203, 249, 166], [116, 249, 45, 207], [176, 129, 177, 16], [212, 117, 104, 159]]
 Number of words (4 bytes each): 44
```

Cipher text:

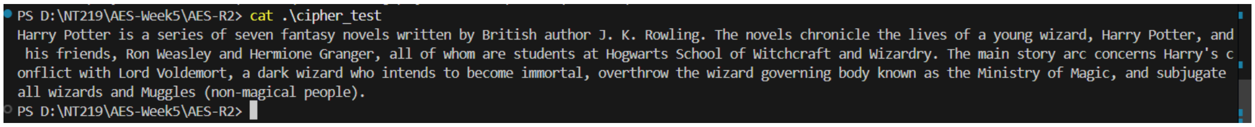


```
PS D:\NT219\AES-Week5\AES-R2> cat .\encrypted

Î»šgû…ü.ûxâÆ¨bÎùds-@¦#PûzR·ü
JD‘bx<PmZºÎ±
+7ëÂOnptp–Ô,iËMÎKÖ‡P¸‡:Œ•¢IañIG:9“,B-©Ù¼ Šé¯•
¤§ë«…dÄço¨Ç<0²aKFÝû2íµýWÿ?e½ô¤«…Öž¤
þø#’g›n¿P¾¼®lÇkÐï,ãi‡§ ž=À· –ú½5®`o÷ßhâi'
1¨~íŒå9èÜ•ýƒ]B5;!,<çN,Dúÿœ-öä‰µ€³B™÷¡É‡ˆ        ó9EJó®‡†•>fçfaIŠS?BÍøoÈ].-‡(FjMÍUtº t,o. ú*¢<úŠaëbéÕà`Çå¥ErjK–äÖÐm"©™"VSð؟©%b¡¹ÎOÉÚør–ñV‰ub«-r¬Ê؟QäÇ¢ºƒM™SîÔ¨
oe+;†2T“›GÚZ²K2Ah¥·ôF1œ0éSyE6£Ëuu€¦EsxÙSø[sêxpÕU©³:Üw;ÆfÑ
Ã©Òô³ó<Ì#µFx}Övð0ŠIÕ²é$öET‘Ú¦BÒ ßP†q±kâ©i¼ôo†Nu[/pÐ¿¥Þ‰L'=.-ËžeþOPá1 Î|Ž×áúšÐ5(ö§l <ð±
PS D:\NT219\AES-Week5\AES-R2> 
```



```
PS D:\NT219\AES-Week5\AES-R2> python .\AES_project.py
Select AES mode:
1. ECB
2. CBC
3. CFB
4. OFB
5. CTR
Enter choice (1/2/3/4/5): 1
Enter to option:
1. Encrypt
2. Decrypt
Enter option(1/2): 2
Enter name file to decrypt: encrypted
Length of file encrypted (bytes):  528
Enter name file to save: cipher_test
Length of cipher_test (bytes):  516


 Extension key for 10 rounds: [[49, 50, 51, 52], [53, 54, 55, 56], [97, 98, 99, 100], [101, 102, 103, 104], [3, 183, 118, 121], [54, 129, 65, 65], [87, 227,
34, 37], [50, 133, 69, 77], [150, 217, 149, 90], [160, 88, 212, 27], [247, 187, 246, 62], [197, 62, 179, 115], [32, 180, 26, 252], [128, 236, 206, 231], [119
, 87, 56, 217], [178, 105, 139, 170], [209, 137, 182, 203], [81, 101, 120, 44], [38, 50, 64, 245], [148, 91, 203, 95], [248, 150, 121, 233], [169, 243, 1, 19
7], [143, 193, 65, 48], [27, 154, 138, 111], [96, 232, 209, 70], [201, 27, 208, 131], [70, 218, 145, 179], [93, 64, 27, 220], [41, 71, 87, 10], [224, 92, 135
, 137], [166, 134, 22, 58], [251, 198, 13, 230], [29, 144, 217, 5], [253, 204, 94, 140], [91, 74, 72, 182], [160, 140, 69, 80], [98, 254, 138, 229], [159, 50
, 212, 105], [196, 120, 156, 223], [100, 244, 217, 143], [235, 203, 249, 166], [116, 249, 45, 207], [176, 129, 177, 16], [212, 117, 104, 159]]
 Number of words (4 bytes each): 44
```

Encrypted text:



```
PS D:\NT219\AES-Week5\AES-R2> cat .\cipher_test
Harry Potter is a series of seven fantasy novels written by British author J. K. Rowling. The novels chronicle the lives of a young wizard, Harry Potter, and
 his friends, Ron Weasley and Hermione Granger, all of whom are students at Hogwarts School of Witchcraft and Wizardry. The main story arc concerns Harry's c
onflict with Lord Voldemort, a dark wizard who intends to become immortal, overthrow the wizard governing body known as the Ministry of Magic, and subjugate
all wizards and Muggles (non-magical people).
PS D:\NT219\AES-Week5\AES-R2> 
```

AES_project.py: NT219-Cryptography/AES-Week5/AES-R2/AES_project.py at main · Duck8605/NT219-Cryptography

modes.py:NT219-Cryptography/AES-Week5/AES-R2/mypackages/modes.py at main · Duck8605/NT219-Cryptography