Zadanie 4

Jedną z operacji w szyfrze AES jest *MixColumns*. Operacja polega na przemnożeniu każdej kolumny stanu przez macierz MDS:

$$\begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix},$$

w ciele $GF(2^8)$ budowanym na podstawie wielomianu nierozkładalnego $x^8 + x^4 + x^3 + x + 1$, gdzie każdy element kolumny identyfikujemy z wielomianem $a(x) = a_7x^7 + a_6x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, dla $a_i \in GF(2)$, natomiast 2 rozumiemy jako x, a 3 jako $x + 1$.

Zadanie polega na implementacji innej macierzy MDS do operacji *MixColumns* :

$$\begin{pmatrix} 2 & 1 & 1 & 1 \\ 1 & 1 & 3 & 2 \\ 1 & 2 & 1 & 3 \\ 1 & 3 & 2 & 1 \end{pmatrix}$$

.

W ścieżce */Dodatki/Zadanie_4* znajduje się plik *aes.py*. Jest to implementacja szyfru aes, w którym należy uzupełnić funkcję *mix_single_column*.

Flagę uzyskasz po zaimplementowaniu funkcji i uruchomieniu kodu - wyświetlony zostanie ciąg bytów, flagą będzie pierwszy bajt np. dla ciągu *b'\x12 \x88'* będzie to: *\x12*.

Podpowiedzi :)

1. Pamiętaj, że

$$x^8 + x^4 + x^3 + x + 1 \equiv_{x^8+x^4+x^3+x+1} 0$$

2. Elementy kolumn stanu to bajty - myśl o nich teoretycznie jako o wielomianach, a w kodzie jako ciągach binarnych

3. Spróbuj pomnożyć 2 (czyli x) przez element kolumny stanu przedstawionej jako wielomian $a(x)$. Następnie pamiętaj, że mnożenie jest w ciele $GF(2^8)$.

4. Spróbuj pomnożyć 3 (czyli x) przez element kolumny stanu przedstawionej jako wielomian $a(x)$.Następnie pamiętaj, że mnożenie jest w ciele $GF(2^8)$. Czy widzisz związek z poprzednim punktem?

5. Zastanów się jakie operacje binarne w pythonie (`https://www.w3schools.com/python/gloss_python_bitwise_operators.asp`) odpowiadają mnożeniu przez 2 i 3.

6. Zastanów się jak użyć operacji binarnych do określenia, czy na danym miejscu ciągu binarnego stoi 1.

7. Zastanów się jak za pomocą operacji binarnych ograniczyć ciągi binarne w pythonie do 8 elementów (jakiej operacji użyć i z jakim ciągiem)

8. Dla uproszczenia możesz w kodzie zamiast liczb używać ciągów binarnych - należy rozpoczynać ciąg od *0b* np. *0b11* to binarne liczba 3.