Problema 1 (10 puntos)

Carol espera que su trabajo de investigación sea del agrado de Aldous, pues depende de su evaluación positiva para poder defender públicamente su Tesis. Aldous ha enviado un mensaje para sus dos colegas, Simon y Melvin, con el resultado. Ella ha podido averiguar por casualidad lo siguiente:

1) El mensaje se ha permutado con la matriz **P=(8 11 5 7 10 2 3 4 1 13 14 6 12 9)**, donde el carácter número 1 del mensaje es el de más a la izquierda, y luego comprimido con un LZW
2) El resultado se ha vuelto a comprimir pero ahora aritméticamente y agrupando los símbolos de 4 en 4
3) El resultado se ha cifrado de la siguiente forma:
    3.1) Simon tiene $\mathbf{n_1=799}$ (17*47, secretos), y Melvin tiene $\mathbf{n_2=667}$ (23*29, secretos) como públicos en ese momento
    3.2) La clave de cifrado es **e=123**, y es pública y compartida por los 3
    3.3) Aldous calcula 2 criptogramas, uno para Simon y es $\mathbf{m^e(mod n_1)=40}$ y otro para Melvin y es $\mathbf{m^e(mod n_2)=65}$
    3.4) El mensaje interceptado es un número en notación octal y que convertido a bits es en realidad el mensaje enviado, esto es, el número real de la compresión aritmética (el MSB es el de más a la izquierda)

Dada esta información privilegiada, ¿podrías ayudar a Carol a resolver los siguientes apartados?

1) (1 punto) ¿Cuál es el mensaje (m_1) recibido en Zn_1?
2) (1 punto) ¿Cuál es el mensaje (m_2) en Zn_2?
3) (1,25 puntos) ¿Cuál es el criptograma en Zn_1*n_2?
4) (1,25 puntos) ¿Cuál es el mensaje (m_3) recibido en Zn_1*n_2?
5) (0,75 puntos) ¿Qué restricción debe tener e para garantizar el funcionamiento?
6) (1,25 puntos) ¿Cuál es el mensaje (m_4) después de la descompresión aritmética de m_3?
7) (1,25 puntos) Da un número en notación octal (m_{3b}) que codifique aritméticamente el mismo mensaje m_4 y que garantice que el código sea instantáneo, ¿m_3 garantiza que sea instantáneo?
8) (1,25 puntos) ¿Cuál es el mensaje (m_5) obtenido después de la descompresión LZW de m_4?, ¿cómo ha quedado el diccionario?
9) (1 punto) ¿Cuál es la permutación inversa a la inicial? , ¿cuál es el mensaje original enviado?

DATOS:

- Diccionario inicial para el LZW más las probabilidades de aparición de los índices y la función de distribución acumulada considerados (podrían ser secretos):

Índice	Palabra	P(Índice)	F(Índice)
1	A	0,0582	0,0582
2	D	0,0718	0,13
3	S	0,0582	0,1882
4	SG	0,0718	0,26
5	I	0,0582	0,3182
6	SGO	0,0718	0,39
7	SGOA	0,0582	0,4482
8	T	0,0718	0,52
9	DE	0,0582	0,5782
10	SGOAT	0,0718	0,65
11		0,0582	0,7082
12		0,0718	0,78
13		0,0582	0,8382
14		0,0718	0,91
15		0,0582	0,9682
16		0,0318	1

- El exponente universal $\lambda\mathbf{(n)}$ es igual a $\mathbf{mcm(}\varphi\mathbf{(f_1),(}\varphi\mathbf{(f_2),\ldots,(}\varphi\mathbf{(f_k))}$ para el módulo $n=f_1*f_2*\ldots*f_k$ cuando f_i $(1<=i<=k)$ es un factor primo impar incluida la multiplicidad del mismo

- Para los apartados 6), 7), 8), y 9) y en el caso de que no se haya conseguido encontrar m_3 tal como propone el problema, considera:
    a) m_3= 43504
    b) La entrada del diccionario 4 como OD, 6 como ODG, 7 como ODGE, 9 como ID y la entrada 10 como ODGEA
    c) La permutación inicial P como (11 1 8 10 7 13 14 2 12 3 4 6 9 5)