Criptografía y Seguridad
Tarea 1

Altamirano Vázquez Jesús Fernando
Rubí Rojas Tania Michelle

14 de marzo de 2020

1. Mostrar que si $(a, n) = 1$, los conjuntos de clases $\{a, 2a, 3a, ..., (n-1)a\} = \{1, 2, ..., n-1\}$ en $\mathbb{Z}_n$.

   Demostración. Supongamos que $(a, n) = 1$. Por hipótesis, sabemos que cada entero es congruente (mód n) a exactamente uno de $a, 2a, 3a, ..., (n-1)a$. Ahora bien, el conjunto $\{a, 2a, 3a, ..., (n-1)a\}$ tiene $n-1$ elementos, y ninguno de ellos es congruente con 0 (mód n), por lo que cada uno de los elementos es congruente (mód n) a uno de los números del conjunto $\{a, 2a, 3a, ..., (n-1)a\}$.

   Debemos mostrar que no hay dos enteros en el conjunto $\{a, 2a, 3a, ..., (n-1)a\}$ que sean congruentes (mód n), ya que se sigue que sus residuos *mínimos* (mód n) son todos diferentes y eso hace que sea igual al conjunto $\{1, 2, ..., n-1\}$.

   Supongamos que hay dos enteros en el conjunto $\{a, 2a, 3a, ..., (n-1)a\}$ que son congruentes (mód n), esto es, $ka \equiv la$ (mód n). Como $(a, n) = 1$, por el teorema

   $$\text{Si } ac \equiv bc \text{ y } (c, n) = d, \text{ entonces } a \equiv b \pmod{\tfrac{m}{d}}$$

   tenemos que $k \equiv l$ (mód n), lo que implica que $k = l$.

   Por lo tanto, $\{a, 2a, 3a, ..., (n-1)a\} = \{1, 2, ..., n-1\}$.

   □

2. Dar las unidades de $\mathbb{Z}_{156}$ y su inverso multiplicativo de la siguiente forma (a, a^{-1}).

   SOLUCIÓN: Sabemos que un elemento a es invertible módulo m si existe a^{-1} en $\mathbb{Z}_m$ tal que $a \cdot a^{-1} = 1$. Decimos que a^{-1} es el inverso de a en Z_m. Una unidad es un elemento x que es invertible módulo m. Para calcular todas las unidades de $\mathbb{Z}_{156}$ lo que hicimos fue implementar el algoritmo extendido de Euclides en Python junto con una función *unidades*() que se encarga de calcular las unidades.

   Para la implementación del AEE simplemente seguimos el procedimiento que se nos enseñó en clase. Ahora bien, para calcular las unidades tuvimos en cuenta el siguiente teorema

   Un entero a es invertible módulo m si y sólo si $(a, m) = 1$. Si a posee inverso, entonces éste es único.

   Para calcular el inverso, entonces lo que hacemos es

   - Aplicamos el AEE para calcular (a, m). Si es diferente de 1, entonces no es invertible. Si es igual a 1, entonces obtenemos la identidad de *Benzout* : $as + mt = 1$.
   - En Z_m, $a \cdot s = 1$, lo que implica que s es el inverso de a módulo m.

   Aplicamos este procedimiento para cada uno de los elementos de $\mathbb{Z}_{156}$, y obtenemos todas las unidades.

```
        '''
        Regresa una tupla (mcd, s, t) que obtenemos al aplicar el algoritmo
        extendido de Euclides, donde as + bt = mcd(a, b) son los elementos que
        conforman la tupla.
        '''
        def aee(a, b):
            s = 0; s_i = 1
            t = 1; t_i = 0
            g = b; g_i = a

            while g != 0:
                cociente = g_i // g
                g_i, g = g, g_i - cociente * g
                s_i, s = s, s_i - cociente * s
                t_i, t = t, t_i - cociente * t

            return (g_i, s_i, t_i)

        # Calcula todas las unidades en Z_{156}.
        def unidades():
            for i in range(0, 156):
                g, s, t = aee(i, 156)
                # El inverso multiplicativo de a modulo m existe sii (a,m) = 1
                if g != 1:
                    continue
                else:
                    inverso = s % 156
                    print("(" + str(i) + ", " + str(inverso) + ")")

        if __name__ == "__main__":
            unidades()

```

Después de ejecutar el programa, obtenemos 48 unidades, las cuales son:

(1, 1)	(5, 125)	(7, 67)	(11, 71)	(17, 101)	(19, 115)
(23, 95)	(25, 25)	(29, 113)	(31, 151)	(35, 107)	(37, 97)
(41, 137)	(43, 127)	(47, 83)	(49, 121)	(53, 53)	(55, 139)
(59, 119)	(61, 133)	(67, 7)	(71, 11)	(73, 109)	(77, 77)
(79, 79)	(83, 47)	(85, 145)	(89, 149)	(95, 23)	(97, 37)
(101, 17)	(103, 103)	(107, 35)	(109, 73)	(113, 29)	(115, 19)
(119, 59)	(121, 49)	(125, 5)	(127, 43)	(131, 131)	(133, 61)
(137, 41)	(139, 55)	(145, 85)	(149, 89)	(151, 31)	(155, 155)

Tabla 1: Unidades en Z_{156}

3. De los siguientes sistemas de congruencias decir si tienen solución, y en caso de tenerla, dar la solución.

   a)

$$\begin{aligned} x &\equiv 10 \pmod{65} \\ x &\equiv 25 \pmod{85} \\ x &\equiv 35 \pmod{70} \\ x &\equiv 15 \pmod{35} \end{aligned}$$

SOLUCIÓN: Por el *Teorema Chino del Residuo* sabemos que un sistema de congruencias lineales tiene solución si y sólo si para cualesquiera $i, j = 1, ..., k, (m_i, m_j) \mid a_i - a_j$; donde m_i, m_j son los módulos y a_i, a_j son los enteros en el lado derecho de la congruencia.
Tenemos que $(65, 85) = 5 \mid -15 = 10 - 25$, $(65, 70) = 5 \mid -25 = 10 - 35$,
$(65, 35) = 5 \mid -5 = 10 - 15$, $(85, 70) = 5 \mid -10 = 25 - 35$, $(85, 35) = 5 \mid 10 = 25 - 15$ pero $(70, 35) = 35 \not\mid 20 = 35 - 15$. Por este último resultado, podemos concluir que el sistema no tiene solución.

b)

$$x \equiv 15 \pmod{35} \tag{1}$$
$$x \equiv 10 \pmod{65} \tag{2}$$
$$x \equiv 25 \pmod{85} \tag{3}$$
$$x \equiv 15 \pmod{145} \tag{4}$$

SOLUCIÓN: Por el *Teorema Chino del Residuo* sabemos que un sistema de congruencias lineales tiene solución si y sólo si para cualesquiera $i, j = 1, ..., k, (m_i, m_j) \mid a_i - a_j$; donde m_i, m_j son los módulos y a_i, a_j son los enteros en el lado derecho de la congruencia.
Tenemos que $(35, 65) = 5 \mid 5 = 15 - 10$, $(35, 85) = 5 \mid -10 = 15 - 25$,
$(35, 145) = 5 \mid 0 = 15 - 15$, $(65, 85) = 5 \mid -15 = 10 - 25$, $(65, 145) = 5 \mid -5 = 10 - 15$ y $(85, 145) = 5 \mid 10 = 25 - 15$. Por lo tanto, el sistema de congruencias tiene solución.
Ahora, resolveremos primero las congruencias (1) y (2). Las soluciones de $x \equiv 15 \pmod{35}$ están dadas por

$$x = 15 + 35y,\ y \in \mathbb{Z} \tag{5}$$

Veamos para cuáles valores de y, x también es solución de la segunda congruencia: sustituimos x en la segunda ecuación y nos queda

$$15 + 35y \equiv 10 \pmod{65}$$

es decir,

$$35y \equiv 10 - 15 = -5 \pmod{65}$$

la cual tiene las mismas soluciones que la congruencia

$$7y \equiv -1 \pmod{13} \tag{6}$$

Dado que 2 es inverso multiplicativo de 7 (mód 13) (ya que $7 \cdot 2 \equiv 1 \pmod{13}$), multiplicando por 2 la congruencia (6) tenemos que

$$y \equiv 11 \pmod{13}$$

por lo que

$$y = 11 + 13z,\ z \in \mathbb{Z} \tag{7}$$

Sustituyendo (7) en (5) obtenemos que conjunto de soluciones simultáneas de las congruencias (1) y (2) es

$$\begin{aligned} x &= 15 + 35(11 + 13z) \\ &= 400 + 455z\ z \in \mathbb{Z} \end{aligned}$$

o, lo que es equivalente

$$x \equiv 400 \pmod{455}$$

Por lo que, el nuevo sistema a resolver es

$$x \equiv 400 \pmod{455} \tag{8}$$
$$x \equiv 25 \pmod{85} \tag{9}$$
$$x \equiv 15 \pmod{145} \tag{10}$$

Postetiormente, resolveremos las congruencias (9) y (10). Las soluciones de $x \equiv 25 \pmod{85}$ están dadas por

$$x = 25 + 85p,\ p \in \mathbb{Z} \tag{11}$$

Veamos ahora para cuáles valores de p, x también es solución de la segunda congruencia: sustituimos x en la segunda ecuación y nos queda

$$25 + 85p \equiv 15 \pmod{145}$$

es decir,

$$85p \equiv 15 - 25 = -10 \pmod{145}$$

la cual tiene las mismas soluciones que la congruencia

$$17p \equiv -2 \pmod{29} \tag{12}$$

Dado que 12 es inverso multiplicativo de 17 (mód 29) (ya que $12 \cdot 17 \equiv 1 \pmod{29}$), multiplicando por 12 la congruencia (12), tenemos que

$$p \equiv 5 \pmod{29}$$

por lo que

$$p = 5 + 29q,\ q \in \mathbb{Z} \tag{13}$$

Sustituyendo (13) en (11) obtenemos que el conjunto de soluciones simultáneas de las congruencias (9) y (10) es

$$\begin{aligned} x &= 25 + 85(5 + 29q) \\ &= -2015 + 2465q,\ q \in \mathbb{Z} \end{aligned}$$

o, lo que es equivalente

$$x \equiv 450 \pmod{2465}$$

Por lo que, el nuevo sistema a resolver es

$$x \equiv 400 \pmod{455} \tag{14}$$
$$x \equiv 450 \pmod{2465} \tag{15}$$

Finalmente, resolvemos las congruencias (14) y (15). Las soluciones de $x \equiv 400$ (mód 455) están dadas por

$$x = 400 + 455r,\ r \in \mathbb{Z} \tag{16}$$

Veamos ahora para cuáles valores de r, x también es solución de la segunda congruencia: sustituimos x en la segunda ecuación y nos queda

$$400 + 455r \equiv 450 \pmod{2465}$$

es decir,

$$455r \equiv 450 - 400 = 50 \pmod{2465}$$

la cual tiene las mismas soluciones que la congruencia

$$91r \equiv 10 \pmod{493} \tag{17}$$

Dado que 428 es inverso multiplicativo de 91 (mód 493) (ya que $428 \cdot 91 \equiv 1$ (mód 493)), multiplicando por 428 la congruencia (17), tenemos que

$$r \equiv 336 \pmod{493}$$

por lo que

$$r = 336 + 493t,\ t \in \mathbb{Z} \tag{18}$$

Sustituyendo (18) en (16) obtenemos que el conjunto de soluciones simultáneas de las congruencias (14) y (15) es

$$\begin{aligned} x &= 400 + 455(336 + 493t) \\ &= 153280 + 224315t,\ t \in \mathbb{Z} \end{aligned}$$

Por lo tanto, la solución del sistema de congruencias original $(1), (2), (3), (4)$ es:

$$x \equiv 153280 \pmod{224315}$$

4. Dado el siguiente texto cifrado

```
ORNOQM PTO ORSO KOLRJFO IOR JNMQSO KJR OL IM PTO GDEO, PTO
OI GOREDAQJQIM. ORSJL OLSQJLGM JI KTLGM GO IJ EQDNSMBQJADJ Y IJ
ROBTQDGJG Y NJQJ JPTOIIMR PTO ORSOL DLSOQORJGMR OL IJ EQDNSMBQ-
JADJ IOR NQMNMLBM PTO AMQKOL TL BQTNM Y ORSO IM GDVDGJL OL
GMR RTUBQTNMR TLM EDAQJQJ Y OI MSQM RTUBQTNM GOREDAQJQJ. OI
QOSM OR OI RDBTDOLSO: OI RTUBQTNM PTO EDAQJ OLEQDNSJ TL KOLRJ-
FO Y IM OLVDJ EDAQJGM J OI RTUBQTNM PTO GOREDAQJ GDEDOLGM PTO
EDAQJGM TRM Y LM KJR DLAMQKJEDML. RD OI BQTNM PTO GOREDAQJ
SQJGTEO OI KOLRJFO RO FTLSJL Y RJEJL EMLEITRDMLOR GO PTO AJISJ
NJQJ KOFMQJQ OI EDAQJGM, OL EJRM EMLSQJQDM OI RTUBQTNM PTO
EDAQJ JNMYJ JI PTO GOREDAQJ NJQJ PTO JVJLEO OI BQTNM. EMKDOLEOL
EML IMR EDAQJGMR KJR ROLEDIIMR EMKM KMLMJIAJUOSDEMR, GORN-
TOR IMR NMIDJIAJUOSDEMR, ITOBM IMR EDAQJGMR OL UIMPTOR EMKM
CDII Y JRD. OR KTY DKNMQSJLSO SOLOQ OL ETOLSJ PTO RML TL BQTNM Y
```

PTO GOUOL JNMYJQRO OLSQO RD. ORSJR NQJESDEJR IOR GJQJL KJGTQOZ
Y OXNOQDOLEDJ, OI RDBTDOLSO NJRM OR DKNIOKOLSJQIM OL IJ VDGJ
EMSDGDJLJ, NMQ OFOKNIM GJGM ETJIPTDOQ JQECDVM, AQJBKOLSJQIM,
EDAQJQIM Y GOFJLGMIM OL OI KDRKM AMQKJSM, GORNTOR IJ NJQSO
PTO GOREDAQJ, DKNIOKOLSJ OI JIBMQDSKM GO GOREDAQJGM GOFJLGM
OI JQECDVM EMKM OI MQDBDLJI. QOETOQGOL PTO OL ORSJ NJQSO OR
KTY DKNMQSJLSO PTO TRSOGOR CJBJL SMGMR IMR NQMBQJKJR SJLSM
NJQJ EDAQJQ EMKM NJQJ GOREDAQJQ, YJ PTO OI METNJQ RMAWJQO GO
SOQEOQMR EMKNQMKOSO SMGM OI SQJUJFM. TLJ VOZ COECM ORSM RO
GJQJL ETOLSJ GO PTO KTECJR NOQRMLJR LOEORDSJL GO RTR ROQV-
DEDMR Y JI CJEOQ ORSJR NQJESDEJR OL OI AMLGM RO ORSJL NQONJQJLGM
KOQEJGM IJUMQJI Y LM EMKM OKNIOJGMR RDLM EMKM OKNQORJQDMR.
IJ VOLSJFJ GO CJEOQIM GO ORSJ KJLOQJ, OR PTO OL OI KOQEJGM JESTJI
IJR NOPTOLJR OKNQORJR LOEORDSJL GO TRSOGOR NJQJ EQOEOQ LOEORDSJLGM
GO TLJ EQDNSMBQJADJ KJR NOQRMLJIDZJGJ Y KOLMR EMKOQEDJI UQDLGJLGM
JRD KJR EMLADJLZJ OL IJR OKNQORJR M NOQRMLJR PTO EMLSQJSJL LTORSQMR
ROQVDEDMR, NMQPTO IJR BQJLGOR OKNQORJR PTO JESTJIKOLSO UQDLGJL
ORO ROQVDEDM CJL AJIIJGM. NMQ OFOKNIM OL OI GMR KDI PTDLEO OI
OREJLGJIM GO ORNDMLJFO NMQ NJQSO GO BMMBIO J NOQRMLJR Y OKN-
QORJR GO IJ EMKTLDGJG OTQMNOJ, IJR ETJIOR QONOQETSDOQML SJLSM
NMIDSDEJKOLSO EMKM OEMLMKDEJKOLSO, ORSO SDNM GO JEMLSOEDK-
DOLSMR JUQO NTOQSJR NJQJ NOQRMLJR EMKM LMRMSQMR YJ PTO IJ GO-
REMLADJLZJ GO IJR BQJLGOR OKNQORJR PTO RO GOGDEJL J IJ ROBTQDGJG
EMKNTSJEDMLJI RO CJ NTORSM OL SOIJ GO FTDEDM, NMQ ORM OR DKNMQSJL-
SO PTO GORGO JCMQDSJ EMKDOLEOL J SQJUJFJQ IJR NOQRMLJR PTO
ORSJL DLSOQORJGJR. LM ROQJ AJEDI, NOQM LJGJ PTO VJIBJ IJ NOLJ OR
AJEDI. RJITGMR Y UDOLVOLDGMR JI ETQRM ORNOQJKMR PTO IM GDRAQT-
SOL.

a) Hacer análisis de frecuencias.

Solución: Realizamos el análisis de frecuencias de cada una de las letras (manualmente) y colocamos los resultados obtenidos en una bonita tabla:

Letra	No. Apariciones	Frecuencia
A	36	1.7 %
B	28	1.3 %
C	12	0.5 %
D	111	5.24 %
E	101	4.7 %
F	14	0.6 %
G	90	4.3 %
H	0	0.0 %
I	99	4.7 %
J	242	11.6 %
K	65	3.1 %
L	134	6.4 %
M	184	8.8 %
N	78	3.7 %
O	294	14.1 %

Letra	No. Apariciones	Frecuencia
P	35	1.6 %
Q	151	7.2 %
R	169	8.1 %
S	87	4.1 %
T	93	4.4 %
U	16	0.7 %
V	13	0.6 %
W	1	0.05 %
X	1	0.05 %
Y	22	1.0 %
Z	5	0.2 %

b) Dar la clave de cifrado.

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
J U E G O A B C D F H I K L M N P R S T U V W X Y Z
```

SOLUCIÓN: Juego

c) Dar la regla de descifrado.

SOLUCIÓN: Tomemos en cuenta las letras más usadas en español

Letra	Frecuencia
E	13.68 %
A	12.53 %
O	8.68 %
S	7.98 %
R	6.87 %
N	6.71 %
I	6.25 %

Realizamos una sustitución de las letras mas usadas del español con las más usadas en el texto, haremos esto en los primeros tres renglones del texto cifrado, de donde obtenemos:

```
ESNERO PTE ESSE KENSAFE IES ANORSE KAS EN IO PTE GIEE, PTE EI
GESEIARARIO. ESSAN ENSRANGO AI KTNGO GE IA ERINSOBRAAIA Y IA
SEBTRIGAG Y NARA APTEIIOS PTE ESSEN INSERESAGOS EN IA ERINSOBRAAIA
```

Entonces

$$\begin{aligned} \mathrm{O} &\to \mathrm{E} \\ \mathrm{J} &\to \mathrm{A} \\ \mathrm{M} &\to \mathrm{O} \\ \mathrm{R} &\to \mathrm{S} \\ \mathrm{Q} &\to \mathrm{R} \\ \mathrm{L} &\to \mathrm{N} \\ \mathrm{D} &\to \mathrm{I} \end{aligned}$$

De este fragmento podemos deducir que

$$\begin{aligned} N &\to P \\ S &\to T \\ K &\to M \\ F &\to J \\ I &\to L \\ G &\to D \\ Y &\to Y \end{aligned}$$

Con esto obtenemos que

```
ESPERO PTE ESTE MENSAJE LES APORTE MAS EN LO PTE DIEE, PTE EL
DESEIARARLO. ESTAN ENTRANDO AL MTNDO DE LA ERIPTOBRAAIA Y LA
SEBTRIDAD Y PARA APTELLOS PTE ESTEN INTERESADOS EN LA ERIPTOBRAAIA
```

Por contexto, deducimos que

$$\begin{aligned} P &\to Q \\ T &\to U \\ E &\to C \\ B &\to G \\ A &\to F \end{aligned}$$

de donde obtenemos

```
ESPERO QUE ESTE MENSAJE LES APORTE MAS DE LO QUE DICE, QUE EL
DESCIFRARLO. ESTAN ENTRANDO AL MUNDO DE LA CRIPTOGRAFIA Y LA
SEGURIDAD Y PARA AQUELLOS QUE ESTEN INTERESADOS EN LA CRIPTOGRAFIA
```

Sustituyendo en el texto tenemos que

$$\begin{aligned} C &\to H \\ U &\to B \\ V &\to B \\ W &\to W \\ X &\to X \\ Z &\to Z \end{aligned}$$

d) Descifrar el mensaje.
SOLUCIÓN:

```
ESPERO QUE ESTE MENSAJE LES APORTE MAS EN LO QUE DICE QUE EL
DESCIFRARLO ESTAN ENTRANDO AL MUNDO DE LA CRIPTOGRAFIA Y LA
SEGURIDAD Y PARA AQUELLOS QUE ESTEN INTERESADOS EN LA CRIPTOGRAFIA
LES PROPONGO QUE FORMEN UN GRUPO Y ESTE LO DIVIDAN EN DOS SUBGRUPOS
UNO CIFRARA Y EL OTRO SUBGRUPO DESCIFRARA EL RETO ES EL SIGUIENTE
EL SUBGRUPO QUE CIFRA ENCRIPTA UN MENSAJE Y LO ENVIA CIFRADO A EL
SUBGRUPO QUE DESCIFRA DICIENDO QUE CIFRADO USO Y NO MAS INFORMACION
SI EL GRUPO QUE DESCIFRA TRADUCE EL MENSAJE SE JUNTAN Y SACAN
CONCLUSIONES DE QUE FALTA PARA MEJORAR EL CIFRADO EN CASO CONTRARIO
EL SUBGRUPO QUE CIFRA APOYA AL QUE DESCIFRA PARA QUE AVANCE EL
GRUPO COMIENCEN CON LOS CIFRADOS MAS SENCILLOS COMO MONOALFABETICOS
DESPUES LOS POLIALFABETICOS LUEGO LOS CIFRADOS EN BLOQUES COMO HILL
```

Y ASI ES MUY IMPORTANTE TENER EN CUENTA QUE SON UN GRUPO Y QUE DEBEN APOYARSE ENTRE SI ESTAS PRACTICAS LES DARAN MADUREZ Y EXPERIENCIA EL SIGUIENTE PASO ES IMPLEMENTARLO EN LA VIDA COTIDIANA POR EJEMPLO DADO CUALQUIER ARCHIVO FRAGMENTARLO CIFRARLO Y DEJANDOLO EN EL MISMO FORMATO DESPUES LA PARTE QUE DESCIFRA IMPLEMENTA EL ALGORITMO DE DESCIFRADO DEJANDO EL ARCHIVO COMO EL ORIGINAL RECUERDEN QUE EN ESTA PARTE ES MUY IMPORTANTE QUE USTEDES HAGAN TODOS LOS PROGRAMAS TANTO PARA CIFRAR COMO PARA DESCIFRAR YA QUE EL OCUPAR SOFWARE DE TERCEROS COMPROMETE TODO EL TRABAJO UNA VEZ HECHO ESTO SE DARAN CUENTA DE QUE MUCHAS PERSONAS NECESITAN DE SUS SERVICIOS Y AL HACER ESTAS PRACTICAS EN EL FONDO SE ESTAN PREPARANDO MERCADO LABORAL Y NO COMO EMPLEADOS SINO COMO EMPRESARIOS LA VENTAJA DE HACERLO DE ESTA MANERA ES QUE EN EL MERCADO ACTUAL LAS PEQUENAS EMPRESAS NECESITAN DE USTEDES PARA CRECER NECESITANDO DE UNA CRIPTOGRAFIA MAS PERSONALIZADA Y MENOS COMERCIAL BRINDANDO ASI MAS CONFIANZA EN LAS EMPRESAS O PERSONAS QUE CONTRATAN NUESTROS SERVICIOS PORQUE LAS GRANDES EMPRESAS QUE ACTUALMENTE BRINDAN ESE SERVICIO HAN FALLADO POR EJEMPLO EN EL DOS MIL QUINCE EL ESCANDALO DE ESPIONAJE POR PARTE DE GOOGLE A PERSONAS Y EMPRESAS DE LA COMUNIDAD EUROPEA LAS CUALES REPERCUTIERON TANTO POLITICAMENTE COMO ECONOMICAMENTE ESTE TIPO DE ACONTECIMIENTOS ABRE PUERTAS PARA PERSONAS COMO NOSOTROS YA QUE LA DESCONFIANZA DE LAS GRANDES EMPRESAS QUE SE DEDICAN A LA SEGURIDAD COMPUTACIONAL SE HA PUESTO EN TELA DE JUICIO POR ESO ES IMPORTANTE QUE DESDE AHORITA COMIENCEN A TRABAJAR LAS PERSONAS QUE ESTAN INTERESADAS NO SERA FACIL PERO NADA QUE VALGA LA PENA ES FACIL SALUDOS Y BIENVENIDOS AL CURSO ESPERAMOS QUE LO DISFRUTEN.

5. Dado el siguiente mensaje cifrado con Vinegere.

```
T S I I C H G D E A  U E F A V V I G S L  M X L G G S X S F A  S G E F R A E A F Q
M W J M Z I P O K R  X A D E K F M X A J  W X E P Q F E S E G  W U S G Z P L A S U
Q V E J M X R Z C Q  Y S Z W P T W E X L  N T A Y S A M N Q M  E Y Z G U Y A Q B H
M O M C L Y A I P L  N W E X B N T A Y Y  B V U U K O P X A G  F F S J C A P W C Y
W Z X R F E L S S Y  I F A T M P X L G S  E C P C N I T D S Q  T I S K P B G G N V
G S A M H X J C G A  V X Y W E U U X X Z  X L Z G S X M Z L Z  F M P D S E I X K G
P C P F J M K J M P  W X E P W N E V M H  M U E G B P X B K C  M X B Z O I F M H L
A W X U Q R G E S P  J E S C Y F C P F J  E S W T I L A W Z W  A Y A S Q Z Q P S D
O W X Q X A V E E N  L U G Z L U D L O G  M Q L B T G I V A I  C U A W X Q F A O O
W U O K N Y P K C N  Z S P M O A S B E O  G J S U Q B A C B A  I K B Q P G P I J W
S K T Q S I G I Z I  E K Q V S I O A K O  Q Q G R J Q D B V N  A S Y X T F A V X E
V U G B Y W E F G R  Y W I G O X X D K O  D S P Q P E K B I O  G E K Q P I Q D R G
U C S Z I K M U T W  W I W U M W J M Z I  T G P I I X Q E E M  V A K N V G H X M N
B Z N O K M Q L Z Q  V Q R C I N T S D Q  K C L D M R B T C M  M K J M P T G H M B
Q P L A C M G D S P  H A N A V F B Q S M  P L Z Q S G Q P J I  N W D E I W D R W D
O J Q W B U K L A A  G Q C Q M Q I K A W  D A W X U Q R G E S  M E E U A Q L C P S
C K U F R V X O O E  P I X K W E J P S X  O B A M R I W U Q M  E O I G L J A W Q Z
G X V G K Z U W Q W  R W X G L V E E H F  Z I J A F P I B V E  H M D E I E E M Z E
W D S A M N A Z M G  Q G N L Q I P K T I  R V X O O E F F S N  P O K Y Y V I E E J
```

```
                                C G H W Y S P T G I  L W Z K R I L E W X  U I F P M L A G L S
F A G S U D M Q W T             M K U G D A M X X U  M U G M U P I M T M  L M N H A Q V O W G
Z S A M G L D A W B             W M F X V F O F M R  M F V V E J Q W M W  X M L V Q L W M K O
S D U F O W U H S Z             S U W Z E Z Q Q E F  W P M A I U E Z M G  D W X M Q M T A L G
T N E F S Y X R G N             B V Q D W E Y I Q D  G I E B E O B K D G  T C B W D M K B Q D
S A M N C M M P P M             M H B C P H W D S B  B O W N L A G R I N  S Z B C V A A T X H
L A V C C G B S E M             R U A E I V W E N A  Z S P               F F I Z Z K O D X S
A L G C Y B D K E F             M N H A Q V O W R A  B A E R A F S O M U  F O W X Q B F K C S
I I T A K K I K U K             E J I T C S D E I W  M P D C P O K P I I  F M T R S K W B X T
Q I P K T I T U V B             U M R B S T O E B M  L I G I B A E R A N  M W L V T R A E E X
S V Q W M M T T G Y             U V W D U R M G M A  M B Q M Q R X K K O  N V Q R L A Q T J A
M Q R A M H B T C M             R T V I E M S Y Z C  S Q W S U W E Y M W  W N A V A R L X W E
S P K W R K A W N C             F M Q C N A V A I I  W E X O I N E S Y S  W A M C L Y Q F O I
Z M V I I N E K B V             E K O V F B Q R W E  U A E A V L A Q S D  L A V F V E O F Y I
K T G E Q B F K C S             R Q O S P S I M E E  K K K O E M W C Q P  U I E N S I W I I S
S D W L J T E E U W             S L T K C W Z G F I  N P B T Q S S Y S O  P W E I S D Q B R Q
O E F L E O M R O J             W D U R M U E W Z G  A T M R A W P A F E  M R A W G L K U K R
I X T I E Q V L L G             Q Y E M W Z I T A D  K Q R S L S K T G S  A F P S S Q V E G D
Z I P O W T A Q V O             A M U C J U T Z Q Q  G R M P T J M R Y C  A W N E M R B R Q D
O H Q V P W P A D Z             F E A I R O J A X O  V A T L L G M G E Z  I P X C N G X I I C
I F O K B E O I O U             E K Y I U Q E A F A  G N L Q P B A K G M  G S V X J K N K W C
X F B W L S P S I W             A J U Y A E I J G R  L B T O W E G O Q V  T E D M R X T K S A
G D I P M N S A X I             S Q I F O I G I I I  Y I O Q F A Z M E N  L V X E J F M A W G
U I F E S M W T T S             G E T B Z O I L Q E  R G F M Q C N A V A  M R Q M U D W F I O
P A Q N D A W N C G             G S L M I P B W D A  U C Y S Q P E M T R  E K E S K A W S S G
Q S I D K D S Z W R             Z W R A J M Q F K W  E J W A L W P M G W
O F F V X Z P O W Z             E Y P T K B J A W B  J M Q X Z E A J M P
```

a) Hacer la prueba de KasisKi describiéndo los pasos para el mensaje.

SOLUCIÓN: Lo primero que debemos hacer para decifrar nuestro texto es averiguar la longitud de la cadena. Al momento de hacer análisis sobre el texto nos damos cuenta de algunas palabras con su número de repeticiones y su longitud. En particular, tenemos que

- Dos cadenas $MKJMPTG$, una de ellas se encuentra en la posición 245 y la otra en la posición 1050.
- Dos cadenas PII en las posiciones 77 y 252.
- Dos cadenas $DURM$ en las posiciones 903 y 1141.

Nos percatamos de que el máximo común divisor de $77, 245, 252, 904, 1050$ y 1141 es 7, entonces la longitud de nuestra cadena probablemente sea de 7.

Ahora haremos 7 subcriptogramas, en donde tomaremos el caracter 0 con el $7, 14, ...$ etc y el 1 con el 8, con el 15, etc. Así, hasta llegar a 6. Entonces

```
[1.] TDBDUFJRALMPMQAQGNAUZQQZSQQZEMDBBE
YMPMPAAEMDXMXNQENYNAEAMEGMQZLUGPFZ
MZRFYAEMEQMQQDZMMEQAAZYMRFCEFAUK
MDQDMEAAPAMMQMMFADDPYEXMBQEYPD
XMMSXMXGUQFADXMGOEACMHPFXUDDZXZBAD
ZKQOAMMEOMZUQAJYFAAQDDYAQAZAAAYQUZG
NPPSEQDXFMMMUQAEMPDXCEAMXEKZXXYQU
USWOQYQMEDMPMFUXABMFDMBAEGMEZ
```

[2.] SEPWWSMEWEPIXLIVIMIQIVRXYDVSYHSIEXS
KIXSVWSRIIWQPPSPSYWSWRSIRSWSGRIVG
RIVSSTZQFMXPPSPFRGWEQEIEVSYYMGWPHSPS
GIEEMVXHVQPMSEEMSXQRMVXIIUM
KPYESMVXPMIMEHHVSTYKMSISDESGQSEQUGWVEW
WWEXDETRWMYEXRRQMIWFVSWEVIIFSIS
ISYTEQGSPIRKIVMQSMSYYWREGIKIISIVPVCP
WMWRCSHMGMFSWERIIVVGSXZQS

[3.] IAXLBOZSZODIRBILBOPBPOXRQBPQMXPOOOP
JIFILXPBPKCXLJMBOPXPNAKZIIRKBZBXR
YKXNPLBLRKXBLPLXLOBYBZONXJBIQXQBBBE
AFXIJGVBLOXXXQJILZLFBLOBKJRL
OXXRYQXXIQIKPVXFZXFJBIZLLILFBPOLRFBSO
QZLXXEAZLIZVAOLCFQUAOFABIFGKOQII
XXXBPBLAPPARPCZFSXFBPBBPIKRPIAPBIXB
XMFMXPQBALAXPNOQOPIBRKLLBP

[4.] IMBJAMIWWMCQZTXLAMLAOMKFQVWWWJQIIICM
XBWAUKTMKQAZIWTWKUACWTIWDKTYIVZMC
MOCTLZZAUUAAWAVBQUZHQQCOCVQCVWGCUM
MMKVWWIZMWZAAZIWAWCASMWNBWMVI
LTTZMYZQCTBWAMBBHCMRMZUOWTIFMMCMMXII
ZIVYDIMQAWIIIWXIAWQMIBMAJVQAWIIWK
TRZWRVMMBWQKCWKQLADTARQIUIXCMKMMJVA
MVWTCMTIVWAKCBMUBIOIAZZF

[5.] CUKTEUPTORPVCGTGECGCWBKEGNPSGCPFONP
PQWUQQCCNKPVQUTQUCQQGPQOUKQGWJEPP
UUOGGGNQEGGKCUSFTVKGSQFKOAQDNGTGPC
TNPGWAUGONREDJQTUGPUOTNGTQUGQF
GFVCTWGDNCQNKNQCJPPQEKGGDKFKOEPUTTOG
QTTWKEUQQUPERNWNGTECHQGJGECWUFUIW
NGOEQENGWGGTGRWVGAKKWQFTKLCN
NTUTKUGTVTKNQCUXGGWGKUKCNWNWGKK

[6.] HECERMOIEOOEQIILRLJBTQOLROAUSGE
OUEFTELASRLMSOOESITSONRNAASBQDRSEAOOT
CTEHIMOSADNGMSUOOOLUUEAUEPDRAKIN
HYRADRELESIHAAEAPCILTAOOHNAPVMLA
SAIDAEERABDENERVEFTOEOZNRCOCAESEREA
LYARIOECNTMOEOAETSEALASLUROQSHOIIE
ENIIRECSDLNIBAAEGLEBNDEALENTQIGMNU
STEESIRMEENERIDDNCENESSTC

```
[7.] GGSEAWKLFJKJMVEIAYSAAMWSJHDWAAKKW
SJGESEDGDGAEWEGFSSKDGDTFIAMSSVFFFWJ
SWFWVGKGFALMGGWFWJAYWFZFFWWGVZSV
WSWZSUNWFLFAJJKYSSFSWWUEAWYGWAWT
AVEWLUKGVWWVVKWASJGSFDLWWWWSSUWWS
KKJEDAGHMJVJWKJJVVSUKFYNMDYLFMDSIESJ
FGLSWHMLAKLLSJFGSGFJEWSKWWGAM
TMGKKVGJDATAWZJEFKEGWSZKLKSXGS
```

Ahora, realizaremos un análisis de frecuencia de cada subcriptograma:

1) Tenemos que

A	$31 - 11\,\%$
B	$7 - 2\,\%$
C	$3 - 1\,\%$
D	$20 - 7\,\%$
E	$22 - 8\,\%$
F	$12 - 4\,\%$
G	$7 - 2\,\%$
H	$1 - 0.3\,\%$
I	$0 - 0\,\%$
J	$2 - 0.7\,\%$
K	$3 - 1\,\%$
L	$2 - 0.7\,\%$
M	$41 - 15\,\%$
N	$5 - 2\,\%$
O	$4 - 1\,\%$
P	$12 - 4\,\%$
Q	$26 - 10\,\%$
R	$3 - 1\,\%$
S	$4 - 1\,\%$
T	$1 - 0.3\,\%$
U	$13 - 4\,\%$
V	$0 - 0\,\%$
W	$1 - 0.3\,\%$
X	$15 - 5\,\%$
Y	$11 - 4\,\%$
Z	$16 - 6\,\%$

2) Tenemos que

A	$0 - 0\,\%$
B	$0 - 0\,\%$
C	$2 - 0.7\,\%$
D	$3 - 1.1\,\%$
E	$23 - 9\,\%$
F	$5 - 2\,\%$
G	$11 - 4\,\%$
H	$6 - 2\,\%$
I	$31 - 11\,\%$
J	$0 - 0\,\%$

K	$5-2\,\%$
L	$1-0.3\,\%$
M	$20-7\,\%$
N	$0-0\,\%$
O	$0-0\,\%$
P	$16-6\,\%$
Q	$12-4\,\%$
R	$15-5\,\%$
S	$39-15\,\%$
T	$4-1\,\%$
U	$2-0.7\,\%$
V	$20-7\,\%$
W	$21-8\,\%$
X	$12-4\,\%$
Y	$11-4\,\%$
Z	$2-0.7\,\%$

3) Tenemos que

A	$31-12\,\%$
B	$7-2\,\%$
C	$3-1\,\%$
D	$20-7\,\%$
E	$22-8\,\%$
F	$12-4\,\%$
G	$7-2\,\%$
H	$1-0.3\,\%$
I	$0-0\,\%$
J	$2-0.7\,\%$
K	$3-1\,\%$
L	$2-0\,\%$
M	$41-15\,\%$
N	$5-2\,\%$
O	$4-1\,\%$
P	$12-4\,\%$
Q	$26-10\,\%$
R	$3-1\,\%$
S	$4-1\,\%$
T	$1-0.3\,\%$
U	$12-4.5\,\%$
V	$0-0\,\%$
W	$1-0.3\,\%$
X	$15-6\,\%$
Y	$11-4\,\%$
Z	$16-6\,\%$

4) Tenemos que

A	$24 - 9\,\%$
B	$11 - 4\,\%$
C	$17 - 6\,\%$
D	$3 - 1\,\%$
E	$0 - 0\,\%$
F	$3 - 1\,\%$
G	$1 - 0.3\,\%$
H	$2 - 0.7\,\%$
I	$28 - 11\,\%$
J	$4 - 1\,\%$
K	$11 - 4\,\%$
L	$5 - 2\,\%$
M	$34 - 13\,\%$
N	$1 - 0.3\,\%$
O	$5 - 2\,\%$
P	$0 - 0\,\%$
Q	$15 - 5\,\%$
R	$4 - 1\,\%$
S	$1 - 0.3\,\%$
T	$14 - 5\,\%$
U	$9 - 3\,\%$
V	$13 - 5\,\%$
W	$31 - 12\,\%$
X	$5 - 2\,\%$
Y	$3 - 1\,\%$
Z	$16 - 6\,\%$

5) Tenemos que

A	$3 - 1\,\%$
B	$1 - 0.3\,\%$
C	$18 - 7\,\%$
D	$4 - 1\,\%$
E	$14 - 5\,\%$
F	$8 - 3\,\%$
G	$39 - 15\,\%$
H	$1 - 0.3\,\%$
I	$1 - 0.3\,\%$
J	$4 - 1\,\%$
K	$21 - 8\,\%$
L	$1 - 0.3\,\%$
M	$0 - 0\,\%$
N	$20 - 7\,\%$
O	$10 - 4\,\%$
P	$17 - 6\,\%$
Q	$25 - 9\,\%$
R	$4 - 1\,\%$
S	$3 - 1\,\%$
T	$22 - 8\,\%$

U	$22-8\,\%$
V	$6-2\,\%$
W	$15-6\,\%$
X	$1-0.3\,\%$
Y	$0-0\,\%$
Z	$0-0\,\%$

6) Tenemos que

A	$27-10\,\%$
B	$5-2\,\%$
C	$9-3\,\%$
D	$10-3\,\%$
E	$42-16\,\%$
F	$2-0.7\,\%$
G	$4-1\,\%$
H	$6-2\,\%$
I	$18-6\,\%$
J	$1-0.3\,\%$
K	$1-0.3\,\%$
L	$15-5\,\%$
M	$8-3\,\%$
N	$16-6\,\%$
O	$25-9\,\%$
P	$3-1\,\%$
Q	$5-1\,\%$
R	$18-7\,\%$
S	$20-7\,\%$
T	$12-4\,\%$
U	$8-3\,\%$
V	$2-0.7\,\%$
W	$0-0\,\%$
X	$0-0\,\%$
Y	$2-0.7\,\%$
Z	$1-0.3\,\%$

7) Tenemos que

A	$20-7\,\%$
B	$0-0\,\%$
C	$0-0\,\%$
D	$10-4\,\%$
E	$13-5\,\%$
F	$22-8\,\%$
G	$24-9\,\%$
H	$3-1\,\%$
I	$3-1\,\%$
J	$19-7\,\%$
K	$20-7\,\%$
L	$11-4\,\%$
M	$10-4\,\%$
N	$2-0.7\,\%$

O	$0 - 0\,\%$
P	$0 - 0\,\%$
Q	$0 - 0\,\%$
R	$0 - 0\,\%$
S	$31 - 12\,\%$
T	$4 - 1\,\%$
U	$5 - 2\,\%$
V	$13 - 5\,\%$
W	$38 - 14\,\%$
X	$1 - 0.3\,\%$
Y	$6 - 2.3\,\%$
Z	$5 - 2\,\%$

Realizando un análisis de cada fragmento obtenemos:

- De 1, vemos que la letra con mayor frecuencia es M.
- De 2, la letra con mayor frecuencia es S, pero MS no tendía mucho sentido, entonces tomamos la vocal con mayor frecuencia, que es E.
- De 3, la mayor frecuencia sobre una letra se presenta en M.
- De 4, vemos que la letra con mayor frecuencia es M, pero necesitamos una vocal, y la que tiene mayor frecuencia es I.
- De 5, observamos que la letra con mayor frecuencia es G.
- De 6, vemos que la letra con mayor frecuencia es A.
- De 7, obervamos que la letra con mayor frecuencia es W, pero ninguna palabra termina con W, entonces tomamos la segunda, que es S.

Observemos como la palabra generada es MEMIGAS, pero eso no tiene mucho sentido, entonces sustituiremos la tercera y quinta letra de la palabra. Al hacer cambios sobre estas dos letras, descubrimos que la palabra clave es MEXICAS.

¿Por qué la palabra clave no es medidas? Esto se da ya que en la quinta posición, esa misma letra tiene una frecuencia muy baja.

b) Dar la clave de cifrado.

Solución: MEXICAS.

c) Descifrar el mensaje.

Solución:

```
HOLA AHORA DESEO PLATICAR SOBRE MIS ESCRITORES MEXICANOS FAVORITOS
COMENZARE POR ALGUNOS DE LITERATURA QUE HE LEIDO EL PRIMERO DEL QUE
ESCRIBIRE ALGO ES DE JAIME SABINES GUTIERREZ QUE NACIO EN TUXCLA
GUTIERREZ EN LO PERSONAL NO TOQUE SU POESIA DABA GIROS INESPERADOS
PARA MUESTRA LEAMOS UN FRAGMENTO DEL POEMA TITULADO LOS AMOROSOS
LOS AMOROSOS CALLAN EL AMOR ES EL SILENCIO MAS FINO EL MAS
TEMBLOROSO EL MAS INSOPORTABLE LOS AMOROSOS BUSCAN LOS AMOROSOS SON
LOS QUE ABANDONAN SON OS QUE CAMBIAN LOS QUE OLVIDAN SU CORAZON LES
DICE QUE NUNCA HAN DE ENCONTRAR NO ENCUENTRAN BUSCAN EN ESTE
FRAGMENTO QUE HEMOS LEIDO PODEMOS VERLOS AMOROSOS BUSCAN E
INMEDIATAMENTE LE SIGUE LOS AMOROSOS SON LOS QUE ABANDONAN OTRO
ESCRITOR ES EMILIO ABREU GOMEZ QUE NACIO EN MERIDA HE AQUI UN
FRAGMENTO MUY PEQUENO DE SU LIBRO TITULADO CANEK HISTORIA Y
LEYENDA DE UN HEROE MAYA EL HERRERO DE LA HACIENDA SE ACERCO AL
NUEVO AMO Y LE DIJO SENOR YA ESTA TERMINADO EL HIERRO PARA MARCAR
```

A LAS BESTIAS HAGO OTRO PARA MARCAR A LOS INDIOS EL AMO CONTESTO USA EL MISMO CANEK ROMPIO EL HIERRO. EN ESTE FRAGMENTO PODEMOS VER QUE EMILIO NO LE AGRADABA LA DESIGUALDAD LA ULTIMA OBRA DE LITERATURA QUE CITARE ES EL LIBRO TITULADO EL LABERINTO DE LA SOLEDAD Y SIN DUDA EL ESCRITOR ES OCTAVIO PAZ HE AQUI UN FRAGMENTO VIEJO O ADOLECENTE CRIOLLO O MEZTIZO GENERAL OBRERO O LICENCIADO EL MEXICANO SE ME APARECE COMO UN SER QUE SE ENCIERRA Y SE PRESERVA MASCARA EL ROSTRO Y MASCARA LA SONRISA AQUI OCTAVIO PAZ HACE UNA DESCRIPCION DE NOSOTROS LOS MEXICANOS MUY ACERTADA POR OTRO LADO NO PUEDEN FALTAR MIS ESCRITORES MEXICANOS DE ALGEBRA FAVORITOS UNO DE ELLOS ES HUGO ALBERTO RINCON MEJIA QUE EN SUS LIBROS HA NOTADO QUE LA SIMBOLOGIA DE ACUERDO AL LENGUAJE NOS PERMITE ASOCIAR MEJOR EL CONCEPTO DEL CUAL SE ESTA ESTUDIANDO EL SIGUIENTE ESCRITOR FUE BASICO PARA MI CUANDO VI TEORIA DE GALOIS Y LO QUE VI EN SUS LIBROS ES UN MANEJO DE LAS IDEAS CLARAS Y EN MI LENGUAJE EL ESPANOL. EL ULTIMO DEL QUE ESCRIBIRE ES GUILLERMO GRABINSKY EN SUS CLASES DESPERTO MI INTERES POR EL ANALISIS Y SU LIBRO TEORIA DE LA MEDIDA SE HA CONVERTIDO EN MI BASE EN LOS CURSOS QUE IMPARTIDO ANTES DE TERMINAR ESTA CHARLA LES PREGUNTO CUALES SON SUS AUTORES FAVORITOS MEXICANOS.

6. Dado el siguiente mensaje cifrado con Hill, del cual se tiene que

IQ SU NF WI FE IY IK CC KO IG UV

proviene de

Como ho ye nd ia es mu yc om un

IQ SU BX EW AF NB CN OD IU BV CG YI OD NF WI FE IY IK CC KO IG UV VD
NB RY BZ EZ YI EL UQ WR IY DG MR NU YY RZ MK KT OH SF AB MW OI ZU
SF US IB EY AO XI CN LB DN EZ CN OT KY XI CA LB XO NB KY LP WD OI YU
HV OM NN AP EM CC KO LH RZ FL IK LH FP IM HJ AN SO MV VD LB CC SL
OQ DF IK RG MU YB PN RZ LH WA SG QK EZ RT KT SO PN WK LH LP EZ RT
YM RR TX KT AN UV WC BX UQ IO VL GS CG OE DF LH NH XJ BX EJ GM BU
AN DF IK RG KS XI CN IK MN QS VC CO SE SW IK IL RT RM OH TX YM RG SO
YM SU GV SO GO WD QG AP CO SO GO OH AN ZP BX QQ UQ SO SC ZR VX UN
PN SF RT MK GO EZ SO IL RT PN SC VD FS AK UI LU SO DJ UV PT TX RZ MK
CC KO LH XJ BX RR GO KJ YG CG SU QQ BG WP AP QS CX WD IK GO UR AN
BX YI ZL JT IK TF PN ZH GM ZH IY KT SF MU IG FL TF YI OD YU HV ZE AN
TX TF JT GO CA CX WC JC CJ GC RZ DJ VD BU GH SO LH JT EJ SW EW OD
RR SC VL ZH IK RT CT CJ YY US SO NF KB PN QQ XI IK LH EW IG FL TF JT
RZ WA OD VH FE UQ EZ TF JV QQ LB ZA SO HV YU VL ZH IK EZ XF YL QG
TX RR CU MU IG AK PN YB RT LH KT YC AN CN GX OI RR CU CG VD LP GH
SF MU OI ZH IG FL TF YI OD OT PT RZ ZL QQ TX KT QT XJ RT IL EY GO IK
OD YG SR EY PT RZ DF AB SO KY ZL CG KY XI SO ME FX GH SR GH SF EG
TX MK PT RZ ZL QQ TX BX VL SY NN IH OG TF SH GM NN VL ZH IK EZ BR
OE CG IQ LB FX GH SF SR GH IX EZ IG EZ SO BR OE IQ GI EY UF GH CN IK
JX ZL YB RR GI IQ YR PN FE CN RR EJ GH NB UQ SO KY ZH OI NN LP GC HV

```
SC PN EY JT FE IK EM DM US OT MU YB PN RZ GO UR AN SF OU AP CW OT
MC CO VD BU AN RT GO WD KJ EZ NH RL YB EZ IK RT SU KY XI ME EW UI
PF CN EY YG SG QK EZ RT PT YM
```

a) Encontrar la matriz de cifrado planteando con cuáles congruencias se obtiene.

SOLUCIÓN: Primero, asociamos cada letra de nuestro alfabeto (supondremos que es de 26 letras, pues quitamos la ñ) con un número, de la forma $(a \to 0, ..., z \to 25)$. Como en la correspondencia anterior solamente aparecen 26 letras, entonces hay que trabajar con los números enteros **módulo 26**.

Ahora, con la información que nos dan como premisa, tenemos las siguientes correspondencias:

$$\begin{bmatrix} I \\ Q \end{bmatrix} = \begin{bmatrix} 8 \\ 16 \end{bmatrix} \mapsto \begin{bmatrix} 2 \\ 14 \end{bmatrix} = \begin{bmatrix} C \\ O \end{bmatrix}$$

$$\begin{bmatrix} S \\ U \end{bmatrix} = \begin{bmatrix} 18 \\ 20 \end{bmatrix} \mapsto \begin{bmatrix} 12 \\ 14 \end{bmatrix} = \begin{bmatrix} M \\ O \end{bmatrix}$$

$$\begin{bmatrix} N \\ F \end{bmatrix} = \begin{bmatrix} 13 \\ 5 \end{bmatrix} \mapsto \begin{bmatrix} 7 \\ 14 \end{bmatrix} = \begin{bmatrix} H \\ O \end{bmatrix}$$

$$\begin{bmatrix} W \\ I \end{bmatrix} = \begin{bmatrix} 22 \\ 8 \end{bmatrix} \mapsto \begin{bmatrix} 24 \\ 4 \end{bmatrix} = \begin{bmatrix} Y \\ E \end{bmatrix}$$

$$\begin{bmatrix} F \\ E \end{bmatrix} = \begin{bmatrix} 5 \\ 4 \end{bmatrix} \mapsto \begin{bmatrix} 13 \\ 3 \end{bmatrix} = \begin{bmatrix} N \\ D \end{bmatrix}$$

$$\begin{bmatrix} I \\ Y \end{bmatrix} = \begin{bmatrix} 8 \\ 24 \end{bmatrix} \mapsto \begin{bmatrix} 8 \\ 0 \end{bmatrix} = \begin{bmatrix} I \\ A \end{bmatrix}$$

$$\begin{bmatrix} I \\ K \end{bmatrix} = \begin{bmatrix} 8 \\ 10 \end{bmatrix} \mapsto \begin{bmatrix} 4 \\ 18 \end{bmatrix} = \begin{bmatrix} E \\ S \end{bmatrix}$$

$$\begin{bmatrix} C \\ C \end{bmatrix} = \begin{bmatrix} 2 \\ 2 \end{bmatrix} \mapsto \begin{bmatrix} 12 \\ 20 \end{bmatrix} = \begin{bmatrix} M \\ U \end{bmatrix}$$

$$\begin{bmatrix} K \\ O \end{bmatrix} = \begin{bmatrix} 10 \\ 14 \end{bmatrix} \mapsto \begin{bmatrix} 24 \\ 2 \end{bmatrix} = \begin{bmatrix} Y \\ C \end{bmatrix}$$

$$\begin{bmatrix} I \\ G \end{bmatrix} = \begin{bmatrix} 8 \\ 6 \end{bmatrix} \mapsto \begin{bmatrix} 14 \\ 12 \end{bmatrix} = \begin{bmatrix} O \\ M \end{bmatrix}$$

$$\begin{bmatrix} U \\ V \end{bmatrix} = \begin{bmatrix} 20 \\ 21 \end{bmatrix} \mapsto \begin{bmatrix} 20 \\ 13 \end{bmatrix} = \begin{bmatrix} U \\ N \end{bmatrix}$$

Recordemos que buscamos la matriz

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad (\text{mód } 26)$$

que hace las transformaciones indicadas arriba sean ciertas. Usando la transformación 6 tenemos que

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 8 \\ 0 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 24 \end{bmatrix} \quad (\text{mód } 26)$$

de donde obtenemos

$$8a + 0b \equiv 8 \pmod{26} \Rightarrow 4a \equiv 4 \pmod{13}$$

$$8c + 0d \equiv 24 \pmod{26} \Rightarrow 4c \equiv 12 \pmod{13}$$

las cuales tienen el mismo conjunto de soluciones que

$$a \equiv 1 \pmod{13}$$

$$c \equiv 3 \pmod{13}$$

Obteniéndo como soluciones

$$a = 1 + 13k, k \in \mathbb{Z} \tag{19}$$
$$c = 3 + 13l, l \in \mathbb{Z} \tag{20}$$

Ahora bien, usando la primer transformación tenemos que

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} 2 \\ 14 \end{bmatrix} \equiv \begin{bmatrix} 8 \\ 16 \end{bmatrix} \pmod{26}$$

de donde obtenemos

$$2a + 14b \equiv 8 \pmod{26} \Rightarrow a + 7b \equiv 7 \pmod{13}$$

$$2c + 14d \equiv 16 \pmod{26} \Rightarrow c + 7c \equiv 6 \pmod{13}$$

Sustituyendo (19) y (20) en las ecuaciones anteriores tenemos que

$$(1 + 13k) + 7b \equiv q \pmod{13}, k \in \mathbb{Z}$$
$$(3 + 13l) + 7c \equiv 3 + 13l, l \in \mathbb{Z}$$

de donde obtenemos

$$7b \equiv 3 \pmod{13}$$
$$7d \equiv 5 \pmod{13}$$

concluyendo que

$$b = 6 + 13m, m \in \mathbb{Z}$$
$$d = 10 + 13n, n \in \mathbb{Z}$$

En particular, si $k = l = m = n = 1$ obtenemos que $a = 14$, $b = 19$, $c = 3$ y $d = 23$. Por lo tanto, la matriz que estamos buscando es

$$\begin{bmatrix} 14 & 19 \\ 3 & 23 \end{bmatrix}$$

b) Calcular la matriz inversa paso a paso.
SOLUCIÓN: Primero, calculamos el determinante de nuestra matriz.

$$\begin{aligned} \det\left(\begin{bmatrix} 14 & -3 \\ -19 & 23 \end{bmatrix}\right) &= 23 \cdot 14 - (-19 \cdot -3) \\ &= 322 - 57 \\ &= 265 \end{aligned}$$

Luego, calculamos la matriz adjunta

$$Ad\left(\begin{bmatrix} 14 & -3 \\ -19 & 23 \end{bmatrix}\right) = \begin{bmatrix} 23 & -3 \\ -19 & 14 \end{bmatrix}$$

Por lo tanto, la matriz inversa es igual a

$$\begin{aligned} \begin{bmatrix} 14 & 19 \\ 3 & 23 \end{bmatrix} &= \frac{1}{265}\begin{bmatrix} 23 & -3 \\ -19 & 14 \end{bmatrix} \\ &= \begin{bmatrix} 15 & 17 \\ 15 & 8 \end{bmatrix} \pmod{26} \end{aligned}$$

c) Descifrar el mensaje.

SOLUCIÓN: Utilizamos el código de nuestro proyecto 1 para poder descifrar el mensaje.

```
COMO DESCUBRIERON SU VOCACION HOY EN DIA ES MUY COMUN POR
INFLUENCIA FAMILIAR POR PROGRAMAS DE TELEVISION PELICULAS E
INTERNET GENERALMENTE EN EL PRIMER MEDIO YA HAY UNA IDEA MUY CLARA
PUES LA FAMILIA NOS EXPONE MUCHO A NUESTRA CARRERA LAS SIGUIENTES
DOS REGULARMENTE SOLO NOS DAN UNA IDEA MUY VAGA CASI NULA PERO
DESPIERTAN NUESTRO INTERES Y LA ULTIMA QUE ES INTERNET NOSOTROS
SOMOS LOS QUE DECIDIMOS QUE TANTO DESEAMOS SABER SOBRE EL TEMA QUE
NOS INTERESA POR LO CUAL NOS DA UN PANORAMA MUY CLARO DE LO QUE
BUSCAMOS EN LA VIDA USTED ES QUE HAN DECIDIDO ESTAR EN CIENCIAS DE
LA COMPUTACION YA HABRAN NOTADO QUE ESTA INVOLUCRADA POR TODOS
LADOS PUES CON LOS AVANCES TECNOLOGICOS HOY PRESENTES LAS
COMPUTADORAS SON FUNDAMENTALES EN ELLOS HAY AVANCES EN
BIOTECNOLOGIA COMO CREAR TELAS DE MANERA BIOLOGICA POR MODELACION
COMPUTACIONAL PARA DISENOS DE PROTEINAS QUE SON USADAS PARA
NUEVOS MEDICAMENTOS O EL MODELO DEL GENOMA PARA DISENO DE VACUNAS
HAY TAMBIEN AVANCES EN FISICA CON EL MODELADO DE FENOMENOS FISICOS
Y ASI PODER ESTUDIARLOS Y COMPRENDERLOS PODRIAMOS MENCIONAR MUCHAS
AREAS DONDE SE APLICA LA CARRERA QUE HAN ELEGIDO Y ALGO IMPORTANTE
QUE DEBEN PENSAR EN ESTE MOMENTO ES CUAL SERA SU SIGUIENTE PASO.
```