Jardines Mendoza César Eduardo
Sánchez Sarmiento Eric
Tarea Criptografía

1.-Mostrar que si (a,n) = 1, los conjuntos de clases {a,2a,3a,....,(n-1)a} = {1,2,3,…,n-1} en Zn.

Hipótesis:

sup (a,n) = 1. y que cada entero es congruente mod n con uno y solo uno de los elementos de **{a, 2a,....,(n-1)a}**
Sabemos que **{a, 2a,....,(n-1)a}** tiene cardinalidad n-1, ninguno de sus elementos es congruente con 0 mod n.
Por lo anterior, sabemos que cada elemento es congruente mod n con uno de los elementos de **{1,2,....,(n-1)} (#).**
PD: No existen 2 enteros ka,ja en {a,2a,.....,(n-1)a} que sean congruentes mod n.
Si sus residuos mínimos mod n son todos diferentes, significa que **(#) = (*).**
. Sup: $\exists$ Ka,Ja ϵ {a,2a,3a,...,(n-1)a} tq Ka $\cong$Ja (mod n).

como (a,n) = 1
usando lo siguiente:
si ac $\cong$ bc y (c,n) = d $\rightarrow$ a $\cong$ b (mod m/d)

Con lo anterior Ka $\cong$ Ja mod n $\rightarrow$ Ka = Ja
$\therefore$ {a, 2a, 3a,...,(n-1)a} = {1,2,3,....,n-1}

2.-Dar las unidades de Z156 y su inverso multiplicativo de la siguiente forma (a, a−1)

Para esto nos apoyamos en el algoritmo de euclides extendido.
Un entero a es invertible módulo m si y sólo si (a, m) = 1. Si a posee inverso, entonces éste es único.
Para cada elemento de Z156 aplicamos lo siguiente:

- Aplicamos el algoritmo extendido de euclides y vemos si (a,m) ≠ 1, si es así entonces no tiene inverso.
  Apliquemoslo en 0.
  (0,156) = 0 entonces no es invertible.
  para 1:
  (1,156) = 1 si es invertible.
- Tomamos que a*s = 1 entonces s es nuestro inverso.
  para 1:
  1*s = 1
  entonces s = 1

Así obtenemos unidad 1 e inverso 1
(1,1)
Aplicamos estos pasos para todos los elementos de Z156.

(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)

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

Sabemos que un sistema de congruencias tiene solución si y sólo si para cualesquiera
i,j ∈ {1,....,K}
(mi, mj) divide a (ai - aj.)
mn = los módulos
an = los enteros

1a)

a) x ~=10 mod(65)
b) x ~=25 mod(85)
c) x ~=35 mod(70)
d) x ~=15 mod(35)

(65,85) = 5 div -15 = 10-25,
(65,70) = 5 div -25 = 10 - 35,
(65,35) = 5 div -5= 10 - 15,
(85,70) = 5 div -10 = 25 -35
(85,35) = 5 div 10 = 25-15
(70,35) = 35 no div 20 = 35 -15
No se cumple la condición pues 35 no divide a 20
por tanto este sistema no tiene solución.

1b)

(a) x ≡ 15 mod 35
(b) x ≡10 mod 65
(c) (x ≡25 mod 85
(d) x ≡15 mod 145

Siguiendo el mismo procedimiento que en el ejercicio anterior:

(35, 65) = 5 div 5 = 15 − 10,
(35, 85) = 5 div − 10 = 15 − 25,
(35, 145) = 5 div 0 = 15 − 15,
(65, 85) = 5 div − 15 = 10 − 25,
(65, 145) = 5 dic − 5 = 10 − 15
(85, 145) = 5 div 10 = 25 − 15.

Se cumple la condición por lo que el sistema se puede resolver.
Resolvemos (a) y (b)
Las soluciones de $x \equiv 15 \bmod 35$ están dadas por

$x = 15 + 35y,\ y \in Z$
Sustituimos x en la segunda congruencia:
$15 + 35y \equiv 10 \pmod{65}$
$35y \equiv 10 - 15 = -5 \pmod{65}$
Esta tiene la misma solución que:
$7y \equiv -1 \pmod{13}$
$7*2 \equiv 1 \bmod 13$
$(7y \equiv -1 \pmod{13}) * 2$
Multiplicamos por 2 pues 2 es inverso multiplicativo de 7 mod 13
Obtenemos: $y \equiv 11 \bmod 13$
$y = 11 + 13z,\ z \in Z$
Sustituimos g en $x = 15 + 35y$,
$x = 15 + 35(11 + 13z)$
$= 400 + 455z,\ z \in Z$
Esto es equivalente a:
$x \equiv 400 \bmod 455$.
El nuevo sistema es:

$x \equiv 400 \bmod 455$ (h)
$x \equiv 25 \bmod 85$ (i)
$x \equiv 15 \bmod 145$(j)

Resolvemos **i** y **j.**
Las soluciones de $x \equiv 25 \bmod 85$ están dadas por:
$x = 25 + 85c,\ c \in Z$
Buscamos los valores para los cuales p y x son solución de la segunda congruencia:
Se sustituye x en la segunda congruencia:
$25 + 85c \equiv 15 \bmod 145$
$= 85 \equiv 15 - 25 = -10 \bmod 145$
La congruencia tiene las mismas soluciones que:
$17c \equiv -2 \bmod 29$

12 es inverso multiplicativo de 17 mod 29
$(12*17 \equiv 1 \bmod 29)$
Si se multiplica $(17c \equiv -2 \bmod 29)$ * 12
se obtiene:
$c \equiv 5 \bmod 29$
entonces
$c = 5 + 29d,\ d \in Z$

Sustituyendo $c = 5 + 29d$ en $x = 25 + 85c$, se obtiene un conjunto de soluciones simultáneas a las congruencias
i, j obtenemos:
$x = 25 + 85\ (5+29d)$

x = -2015 + 2465d, d∈ Z
= x ≡ 450 mod 2465
Nuestro nuevo Sistema es:

x ≡ 400 mod 455 (n)
x ≡ 450 mod 2465(o)

Resolvemos las congruencias **n,o**
Las soluciones de x ≡ 400 mod 455
están dadas por
x = 400 + 455r, r ∈ Z
Repetimos el procedimiento de buscar los valores de r y x que también son solución de la segunda congruencia, sustituyendo x en la segunda ecuación nos da:
400 + 455r ≡ 450 mod 2465
= 455r ≡ 450 - 400 = 50 mod 2465
Esta tiene la misma solución que la congruencia:
91r ≡ 10 mod 493
(91r ≡ 10 mod 493) * 428
428 es inverso multiplicativo de 91 mod 493 pues 428 * 91 ≡ mod 493.
r ≡ 336 mod 493
r= 336 mod 493t, t ∈ Z
Sustituyendo r= 336 mod 493t en x = 400 + 455r obtenemos el conjunto de soluciones de las congruencias **n, o**
x = 400 + 455(336 + 493t)
= 153280 + 224315t, t ∈ Z
Así obtenemos la solución final
a,b,c,d
x ≡ 153280 mod 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 KJGTQOZY 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 NJQSOPTO GOREDAQJ, DKNIOKOLSJ OI JIBMQDSKM GO GOREDAQJGM GOFJLGMOI JQECDVM EMKM OI MQDBDLJI. QOETOQGOL PTO OL ORSJ NJQSO ORKTY DKNMQSJLSO PTO TRSOGOR CJBJL SMGMR IMR NQMBQJKJR SJLSMNJQJ 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 GDRAQTSOL

Haciendo un **análisis de frecuencia** de las palabras usando un algoritmo para buscar y sacando su porcentaje obtenemos que:

Letra	Frecuencia	Porcentaje
O	294	14.01
J	242	11.53
M	184	8.77
R	169	8.05
Q	151	7.19
L	134	6.38
D	111	5.29
E	101	4.81
I	99	4.72
T	94	4.48
G	90	4.29
S	87	4.14
N	78	3.72
K	65	3.10
A	36	1.72
P	35	1.67
F	31	1.48
B	28	1.33
Y	22	1.05
U	16	0.76
V	13	0.62

C	12	0.57
Z	5	0.24
W	1	0.05
X	1	0.05
H	0	0.00

Tabla A

Usaremos como **clave de cifrado JUEGO**, solo basta con acomodar juego con J = A, U = B, C = E, D = G, E = O, F = A, G = B, i.e acomodar la JUEGO en las primeras letras y después su letra cifrada consecutiva así como el ejemplo:

Original	Cifrada
J	A
U	B
E	C
G	D
O	E
A	F
B	G
C	H
D	I
E	C
F	J
G	D
H	K
I	L
J	A
K	M

L	N
M	O
N	P
O	E
P	Q
Q	R
R	S
S	T
T	U
U	B
V	V
W	W
X	X
Y	Y
Z	Z

El color rojo termina siendo la **regla de descifrado**

Dada nuestra tabla de porcentajes sacada del texto cifrado podemos compararla con las letras más usadas (hablando en porcentajes) más usadas.
Las letras más usadas en el español son:

Letra	Porcentaje
E	13.68
A	12.53
O	8.68
S	7.98
R	6.87
N	6.71

I	6.25
D	5.86
L	4.97
C	4.68
T	4.63
U	3.93
M	3.15
P	2.51
B	1.42
G	1.01
V	0.90
Y	0.90
Q	0.88
H	0.70
F	0.69
Z	0.52
J	0.44
Ñ	0.31
X	0.22
K	0.02
W	0.01

Tabla B

Si intercambiamos el valor de la tabla A fila 1 con el valor de la tabla B fila 1 i.e e.i E = O, A = J, O = M, S = R, etc.Y así sucesivamente con las primeras diez letras obtendremos la tabla con el mensaje:

Cifrada	Normal
E	O

A	J
O	M
S	R
R	Q
N	L
I	D
D	E
L	I
C	T

y con esa tabla podemos empezar a descifrar el texto:

ESNERO PTE ESSE **KENSAFE** CES **ANORSE** KAS EN CO **PTE** GILE, PTE EC GESLIARARCO. ESSAN ENSRANGO AC KTNGO GE CA LRINSOBRAAIA Y CA SEBTRIGAG Y **NARA** APTECCOS PTE ESSEN **INSERESAGOS** EN CA LRINSO-BRAAIA CES NRONONBO PTE AORKEN TN BRTNO Y ESSE CO GIVIGAN EN GOS STUBRTNOS TNO LIARARA Y EC OSRO STUBRTNO GESLIARARA. EC RE- SO ES EC SIBTIENSE: EC STUBRTNO PTE LIARA ENLRINSA TN KENSAFE Y **CO ENVIA** LIARAGO A EC STUBRTNO PTE GESLIARA GILIENGO PTE LIARA-GO TSO Y NO KAS INAORKALION. SI EC BRTNO PTE GESLIARA SRAGTLE EC KENSAFE SE FTNSAN Y SALAN LONLCTSIONES GE PTE AACSA NARA KEFORAR EC LIARAGO, EN LASO LONSRARIO EC STUBRTNO PTE LIARA ANOYA AC PTE GESLIARA NARA PTE AVANLE EC BRTNO. LOKIENLEN LON COS LIARAGOS KAS SENLICCOS LOKO KONOACAAUESILOS, GESNTES COS NOCIACAAUESILOS, CTEBO COS LIARAGOS EN UCOPTES LOKO CICC Y ASI. ES KTY IKNORSANSE SENER EN LTENSA PTE SON TN BRTNO Y PTE GEUEN ANOYARSE **ENSRE** SI. ESSAS NRALSILAS CES GARAN KAGTREZ Y **EXNERIENIA**, EC SIBTIENSE NASO ES IKNCEKENSARCO EN CA VIGA LOSIGIANA, NOREFEKNCO GAGO LTACPTIER ARLCIVO, ARABKENSARCO, LIARARCO Y GE- FANGOCO EN EC KISKO AORKASO, GESNTES CA NARSE PTE GESLIARA, IKN- CEKENSA EC ACBORISKO GE GESLIARAGO GEFANGO EC ARLCIVO LOKO EC ORIBINAC. RELTERGEN PTE EN ESSA NARSE ES KTY IKNORSANSE PTE TS- SEGES CABAN SOGOS COS NROBRAKAS SANSO NARA LIARAR LOKO NARA GESLIARAR, YA PTE EC OLTNAR SOAWARE GE SERLEROS LOKNROKESE SO- GO EC SRAUAFO. TNA VEZ CELCO ESSO SE GARAN LTENSA GE PTE KTLCAS **NERSONAS** NELESISAN GE STS SERVILIOS

Y AC CALER ESSAS NRALSILAS EN EC AONGO SE ESSAN NRENARANGO KERLAGO CAUORAC Y NO LOKO EKNCEAGOS SINO LOKO EKNRESARIOS. CA VENSAFA GE CALERCO GE ESSA KANERA, ES PTE EN EC KERLAGO ALSTAC CAS NEPTENAS EKNRESAS NE- LESISAN GE TSSEGES NARA LRELER NELESISANGO GE TNA LRINSOBRAAIA KAS **NERSONACIZAGA** Y KENOS LOKERLIAC URINGANGO ASI KAS LONAIAN- ZA EN CAS EKNRESAS O NERSONAS PTE LONSRASAN NTESSROS SERVILIOS, NORPTE CAS BRANGES EKNRESAS PTE ALSTACKENSE URINGAN ESE SER- VILIO CAN AACCAGO. NOR EFEKNCO EN EC GOS KIC PTINLE EC ESLAN- GACO GE ESNIONAFE NOR NARSE GE BOOBCE A NERSONAS Y EKNRESAS GE CA LOKTNIGAG ETRONEA, CAS LTACES RENERLTSIERON SANSO NOCISI- LAKENSE LOKO ELONOKILAKENSE, ESSE SINO GE ALONSELIKIENSOS AURE NTERSAS NARA NERSONAS LOKO **NOSOSROS** YA PTE CA GESLONAIANZA GE CAS BRANGES EKNRESAS PTE SE GEGILAN A CA SEBTRIGAG LOKNTSA- LIONAC SE CA NTESSO EN SECA GE FTILIO, NOR ESO ES IKNORSANSE PTE GESGE ACORISA LOKIENLEN A SRAUAFAR CAS NERSONAS PTE ESSAN IN- SERESAGAS. NO SERA AALIC, NERO NAGA PTE VACBA CA NENA ES AALIC. SACTGOS Y UIENVENIGOS AC LTRSO ESNERAKOS PTE CO GISARTSEN.

Hemos visto que al cambiar ciertas palabras (con nuestra tabla de 10 letras normales a cifradas) que más se usan en español por la tabla de porcentajes del texto cifrado obtenemos un texto que tiene más significado, también podemos observar que hay palabras que tienen similitud con otras, tanto significado como la longitud de la misma:

KENSAFE = Mensaje

ANORSE = Aporte

PTE = Que

NARA = Para

NERSONACIZAGA = Personalizada

NERSONAS = Personas

ENSRE = Entre

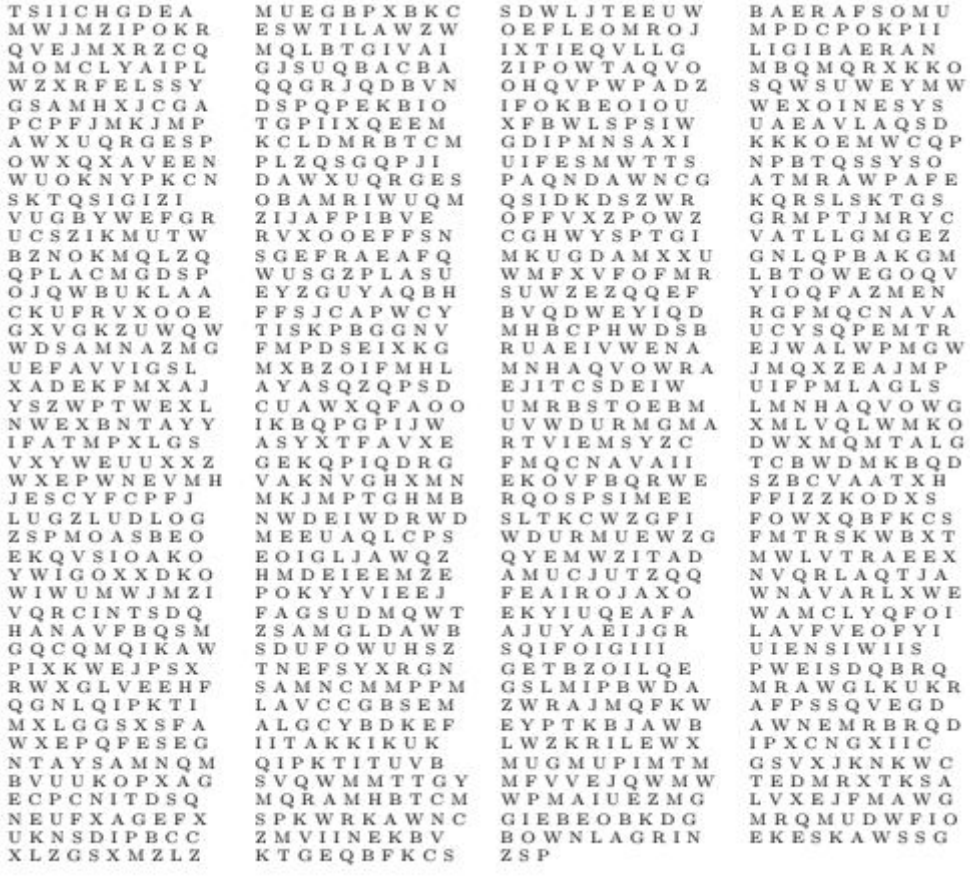
CO = Lo

donde en palabras como NARA podemos deducir que N = P, Kensafe la K = M y F=J, CO con C = L, S=T, etc. Es así como podemos ir viendo que empezamos a crear una **asociación de palabras**, comparando y teniendo un conjunto de estas palabras podemos ir ejecutando una y otra vez para que se pueda descifrar poco a poco el texto, una forma de algoritmo que podríamos usar es en un array, lista o diccionario e ir almacenando estas asociaciones o coincidencias que vayamos encontrando, con for's ir checando si la letra de la posición i es igual a la del nuevo diccionario (algo asi como lo que hicimos con las tablas de porcentajes de letras), ejecutar ya contemplando esas palabras e ir jugando con las nuevas que aparezcan y asociarlas, esto puede tardar un par de pasos ya que no hace falta la palabra que aún no se descifra bien pero ya toma algún sentido**,** así podemos ir encontrando y acercándonos al texto y comparar palabras semejantes hasta dar con el texto final:

ESPERO QUE ESTE MENSAJE LES APORTE MAS EN LO QUE DICE, QUE EL DES- CIFRARLO. ESTAN ENTRANDO AL MUNDO DE LA CRIPTOGRAFIA Y LA SEGURI- DAD 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 INFORMA- CION. SI EL GRUPO QUE DESCIFRA TRADUCE EL MENSAJE SE JUNTAN Y SACAN CONCLUSIONES DE QUE FALTA PARA MEJORAR EL CIFRADO, EN CASO CONTRA- RIO EL SUBGRUPO QUE CIFRA APOYA AL QUE DESCIFRA PARA QUE AVANCE EL GRUPO. COMIENCEN CON LOS CIFRADOS MAS SENCILLOS COMO MONOALFA- BETICOS, 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 COTIDIA- NA, POR EJEMPLO DADO CUALQUIER ARCHIVO, FRAGMENTARLO, CIFRARLO Y DEJANDOLO EN EL MISMO FORMATO, DESPUES LA PARTE QUE DESCIFRA, IM- PLEMENTA EL ALGORITMO DE DESCIFRADO DEJANDO EL ARCHIVO COMO EL ORIGINAL. RECUERDEN QUE EN ESTA PARTE ES MUY IMPORTANTE QUE USTE- DES HAGAN TODOS LOS PROGRAMAS TANTO PARA CIFRAR COMO PARA DES- CIFRAR, YA QUE EL OCUPAR SOFWARE DE TERCEROS COMPROMETE TODO EL TRABAJO. UNA VEZ HECHO ESTO SE DARAN CUENTA DE QUE MUCHAS PERSO- NAS NECESITAN DE SUS SERVICIOS Y AL HACER ESTAS PRACTICAS EN EL FONDO SE ESTAN PREPARANDO MERCADO LABORAL Y NO COMO EMPLEADOS SINO CO- MO 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 PERSO- NAS Y EMPRESAS DE LA COMUNIDAD EUROPEA, LAS CUALES REPERCUTIERON TANTO POLITICAMENTE COMO ECONOMICAMENTE, ESTE TIPO DE ACONTECI- MIENTOS ABRE PUERTAS PARA PERSONAS COMO NOSOTROS YA QUE LA DES- CONFIANZA DE LAS GRANDES EMPRESAS QUE SE DEDICAN A LA SEGURIDAD COMPUTACIONAL SE HA PUESTO EN TELA DE JUICIO, POR ESO ES IMPORTAN- TE QUE DESDE AHORITA COMIENCEN A TRABAJAR LAS PERSONAS QUE ESTAN INTERESADAS. NO SERA FACIL, PERO NADA QUE VALGA LA PENA ES FACIL. SA- LUDOS Y BIENVENIDOS AL CURSO ESPERAMOS QUE LO DISFRUTEN.

5.- Dado el siguiente mensaje cifrado con Vinage.



PALABRA	REPETICIONES	DISTANCIAS	FACTORIZACIÓN
AQVO	2	637, 91	((7^2) *13), (7*13)
SAMN	2	728, 154	(2^3 * 7*13),(2*7*11)
ZIPO	2	96, 1108	(2^3 * 7*13),(2*7*11)
NAVA	2	308, 287	(2^2*7*11),(7*41)
CQMQ	1	1274	2*7^2*13
MZIP	1	1204	2^2 *7*43
BAER	1	84	2^2*3*7
MWJM	1	1204	2^2 *7*43
WJMZ	1	1204	2^2 *7*43
EAMU	1	1211	7*173
AERA	1	84	2^2 * 3 * 7
UMWJ	1	1204	2^2 *7*43
IPOK	1	1204	2^2 *7*43
TILA	1	1435	5*7*41
JMZI	1	1204	2^2 *7*43

Teniendo el análisis y la **prueba Kasiski (la de arriba)** que podemos notar al final de todos los números es que hay algunos que se repiten más que otros como lo son el 2, 3 y 7. Tomaremos al número más grande para ir de ascendente a descendente ya que si empezamos al revés podríamos notar que las llaves serían algo absurdas ya que son pequeñas. Ahora tomando al 7 como decíamos podemos empezar a dar la clave de cifrado, los sub criptogramas se generarán si asumimos que la llave 7 es correcta.

Probaremos dar la **clave de cifrado**

TSIICHG
RESWTIL
AIIXTIE
QVOMBQM
EYMWGSA
MKJMPTG
MRBTCMG
ESMWTTS
MRAWPAF
UGBYWEF
RVXOOEF
QMKUGDA
MRLBTOW
MENCKUF
UWQWTIS
EIXKGRU
QVOWRAJ
PMLAGLS
EXBNTAY
SYXTFAV
FMQCNAV
ESZBCVA
XSLUGZL
BEOMEEU
AWQZQYE
UTZQQNV
ARLXWEV
AVFBQSM
UFOWUHS
ETBZOIL
MRAWGLK
DMXLGGS
EGIITAK

UVBMUGM
QWMWTED
FMAWGNE
DIPBCCZ
EQBFKCS
DEAMUEG
AWZWOEF

QVLLGLI
QRXKKOW
MHXJCGA
PIIXQEE
DIPMNSA
NPBTQSS
ESKTQSI
GRZIJAF
FSNCGHW
MXXUGNL
EGOQVOJ
RVXOOEF
KPBGGNV
AEIVWEN
MQXZEAJ
YSZWPTW
YIKBQPG
XERTVIE
AIITCBW
ATXHJES
UDLOGNW
AQLCPSW
MWZITAD
QRLAQTJ
QRCINTS
ZSAMGLD
ZSQIFOI
QEPWEIS
UKRQGNL
XSFAALG
KIKUKLW
UPIMTMG
MRXTKSA

UFXAGEF
MVIINEK
ZSP
BPXBKCS
LEOMROJ
GIBAERA
ZXRFELS
DSPQPEK
MXFBWLS
XIKKKOE
YSOWUOK
GIZIOBA

PIBVEOF
YSPTGIV
QPBAKGM
QWBUKLA
FSJCAPW
MHBCPHW
AEJWALW
MPXADEK
EXLCUAW
PIJWUVW
MSYZCDW
DMKBQDW
CYFCPFJ
DEIWDRW
DURMUEW
MWLVTRA
AWIWUMW
DQFAGSU
AWBAJUY
GIIIUIE
DQBRQRW
QIPKTIL
CYBDKEF
ZKRILEW
SVXJKNK
ECPCNIT
XSPKWRK
BVBOWNL
DWLJTEE
MPDCPOK
NMOMCLY
SYQQGRJ
BIOIFOK

PSIWUAE
MWCQPOW
NYPKCND
MRIWUQM
FVXZPOW
ATLLGMG
QPLACMG
AEYZGUY
CYBVQDW
DSBUCYS
PMGWUEF
FMXAJAY

XQFAOOU
DURMGMA
XMQMTAL
XEPWNEV
MKJMPTG
DSLTKCW
ZGFMTRS
EEXYWIG
JMZIPOK
DMQWTEK
AEIJGRL
NSIWIIS
XGLVEEH
AVCCGBS
EYPTKBJ
XIPXCNG
WCBVUUK
DSQMQRA
AWNCGIE
AGRINEK
UWBAERA
PIIQVEJ
AIPLGJS
QDBVNOH
BEOIOUW
AVLAQSD
XQXAVEE
AWXUQRG
QSIDKDS
ZGRMPTJ
EZBZNOK
DSPWUSG

AQBHSUW
EYIQDRG
QPEMTRW
AVVIGSL
ASQZQPS
MRBSTOE
XMLVQLW
GVXYWEU
MHVAKNV
HMBRQOS
ZGFIFOW
KWBXTEK
OXXDKOH

Sacando los sub criptogramas dados tomaremos a subs 1, subs2, sub3 … sub7 de la siguiente manera:

subs1: TRAQEMMEMURQMMUEQPESFEXBAUAAUEMDEUQFDE

subs2:DAQQMPDNEGFMERKAMYYXAAUAMQQZZQUXKUMUMZ

subs3: BLGZDMXYGPYQQFMAMEPMDCDDMADAGDQCZSEXB

subs4: DMNSBPMNMFAQACDPFXDXXMDZEJDANXAEXWDAA

subs5: UPAQBAXAQZEDAEQAAMXGMHZKOYYAPFEAXOMBE

subs6: FMUQEANEZMMZZFDMDBMUGPXQMFAYPMMMYQPMG

subs7: JQZZYEQALZEMYAMMDQMQOFZOZAQQSMPXQYMFM

Haciendo un análisis de frecuencia por letra, en la primera columna la letra que más se repite es la M.
En la segunda columna son la R, S, E.
En la tercera: B,L,X
Cuarta columna: T,I,M
Quinta columna: P,G,C
Sexta columna: A,E,N
Séptima columna: S

Con estas letras debemos formar una palabra.
Después de jugar con las palabras, formamos la palabra
Mexicas.

Para **Descifrando el mensaje** la clave será útil y esta debe de cumplir la propiedad de que se repita tantas veces como la longitud de la cadena del mensaje, esto sucede que para cada letra de nuestro mensaje cifrado a esta le tenemos que aplicar su operación inversa que vendría siendo representada por:

$$M_i = C_i - K_i mod(26)$$

M es la letra del mensaje descifrado, C es la letra de nuestro texto ya cifrado y K es la letra de la llave que se usa para descifrar. Aplicando el procedimiento en el texto usando la clave ya antes mencionada tenemos que el mensaje es:

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 LOS QUE CAMBIAN LOS QUE OLVIDAN SU CORAZON LES DICE QUE NUNCA HAN DE ENCONTRAR NO ENCUENTRAN BUSCAN EN ESTE FRAGMENTO QUE HEMOS LEIDO PODEMOS VER LOS AMOROSOS BUSCAN E INMEDIATAMENTE LE SIGUE LOS AMOROSOS SON LOS QUE ABANDONAN OTRO ESCRITOR ES EMILIO ABREU GOMEZ QUE NACIO EN MERIDA HA 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 SEMA APARECE COMO UN SER QUE SE ENCIERRA Y SE PRESERVA MAS CARA EL ROSTRO Y MAS CARA LA SONRRISA 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 GRABIN SKY 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

C=2 0=14 M=12 O=14 H=7 O=14 Y=24 E=4 N=13 D=3 I=8 A=0 E=4 S=18 M=12 U=20 Y=24 C=2 O=14 M=12 U=20 N=13
I=8 Q=16 S=18 U=20 N=13 F=5 W=22 I=8 F=5 E=4 I=8 Y=24 I=8 K=10 C=2 C=2 K=10 O=14 I=8 G=6 U=20 V=24

Teniendo algunos valores cifrados de algunas palabras, tendremos que encontrar cuatro valores los cuales serían a,b,c,d. Iremos aplicando el método de criptoanálisis visto en clase. Tomaremos a I = 8 y A = 0 con sus respectivos correspondientes I = 8 y Y = 24, todo eso por mod 26 sin contar la ñ.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 8 \\ 0 \end{pmatrix} = \begin{pmatrix} 8 \\ 24 \end{pmatrix} mod 26$$

Utilizamos a I y A por qué al multiplicar bx0 y dx0 nos quedamos con a y c, además cumple las propiedades que vimos en la clase y esto es lo que queremos. Resolviendo las congruencias nos quedaría algo del estilo:

$$8a \equiv 8(mod 26)$$
$$8c \equiv 24(mod 26)$$

y justo sacando al 8 de a y c. Y resolviendo las respectivas soluciones nos queda algo de la forma:

$$a = 1 + 13K_1$$
$$c = 3 + 12k_2$$

donde nuestras K1, K2, K3 y K4 (en este caso K1 y K2) pueden tomar valores de 0 y 1. Encontrado a y c, falta por encontrar b y d, esto se puede hacer tomando dos letras con sus respectivos correspondientes así como lo hicimos al inicio.

Tomaremos a C = 2 y O=14 con sus respectivos correspondientes I=8 Q = 16, todo eso por mod 26 sin contar la ñ.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 \\ 14 \end{pmatrix} = \begin{pmatrix} 8 \\ 16 \end{pmatrix} mod 26$$

Sacando sus congruencia podemos ver que nos queda algo del estilo:

$$2a + 14b \equiv 8(mod26)$$
$$2c + 14d \equiv 16(mod26)$$

Lo cual sacando una equivalencia obtendremos que:

$$a + 7b \equiv 4(mod13)$$
$$c + 7d \equiv 8(mod13)$$

Como lo que queremos es sacar el valor de b y d tendremos que hacer las operaciones necesarias para obtenerlas ya que a y c ya las tenemos.

$$(1 + 13k_1) + 7b \equiv 4(mod13)$$
$$(3 + 13k_2) + 7d \equiv 8(mod13)$$

simplificando obtendremos que:

$$7b \equiv 3(mod13)$$
$$7d \equiv 5(mod13)$$

y obteniendo el valor de b y d así como lo hicimos con a y c obtendremos que:

$$b = 6 + 13k_3$$
$$d = 10 + 13k_4$$

donde de igual forma K3 y K4 pueden valer 0 y 1, esto es importante ya que con esto podemos deducir que las variables tienen al menos dos valores y lo vemos de la siguiente manera:

$$a = 1\ i.e\ a = 1 + 0$$
$$a = 14\ i.e\ a = 1 + 13$$
$$b = 1\ i.e\ b = 6 + 0$$
$$b = 14\ i.e\ b = 6 + 13$$
$$c = 1\ i.e\ c = 3 + 0$$
$$c = 14\ i.e\ c = 3 + 13$$
$$d = 1\ i.e\ d = 10 + 0$$
$$d = 14\ i.e\ d = 10 + 13$$

Entonces demostrado eso, sabemos que a puede valer 1 o 14, b puede valer 6 o 19, c puede valer 3 o 16 y d puede valer 10 o 23. Al tener diferentes valores nos dice que existen varias combinaciones de matrices, sacando dichas matrices nos enfocaremos en la de [[1,6],[3,23]].

Entonces si sacamos los resultados de la matriz ([1,6], [3,23]) es para cifrar y obtenemos su inversa es:

$$\begin{pmatrix} 1 & 6 \\ 3 & 23 \end{pmatrix}^{-1} = \frac{1}{5}\begin{pmatrix} 23 & -3 \\ -6 & 1 \end{pmatrix}^{T} = 21\begin{pmatrix} 23 & -6 \\ -3 & 1 \end{pmatrix}(mod26) = \begin{pmatrix} 15 & 4 \\ 15 & 21 \end{pmatrix}$$

donde obtenemos como resultado la matriz 2x2 nos ayuda desencriptar cualquier mensaje que:

$$\begin{pmatrix} 15 & 4 \\ 15 & 21 \end{pmatrix}$$

Y con esa matriz de 2x2 podemos desencriptar el mensaje:

co mo de sc ub ri er on su vo ca ci on ho ye nd ia es mu yc om un po ri nf lu en ci af am il ia rp or pr og ra ma sd et el ev is io np el ic ul as ei nt er ne tg en er al me nt ee ne lp ri me rm ed io ya ha yu na id ea mu yc la ra pu es la fa mi li an os ex po ne mu ch oa nu es tr ac ar re ra la ss ig ui en te sd os re gu la rm en te so lo no sd an un ai de am uy va ga ca si nu la pe ro de sp ie rt an nu es tr oi nt er es yl au lt im aq ue es in te rn et no so tr os so mo sl os qu ed ec id im os qu et an to de se am os sa be rs ob re el te ma qu en os in te re sa po rl oc ua ln os da un pa no ra ma mu yc la ro de lo qu eb us ca mo se nl av id au st ed es qu eh an de ci di do es ta re nc ie nc ia sd el ac om pu ta ci on ya ha br an no ta do qu ee st ai nv ol uc ra da po rt od os la do sp ue sc on lo sa va nc es te cn ol og ic os ho yp re se nt es la sc om pu ta do ra ss on fu nd am en ta le se ne ll os ha ya va nc es en bi ot ec no lo gi ac om oc re ar te la sd em an er ab io lo gi ca po rm od el ac io nc om pu ta ci on al pa ra di se no sd ep ro te in as qu es on us ad as pa ra nu ev os me di ca me nt os oe lm od ad od el ge no ma pa ra di se no de va cu na sh ay ta mb ie na va nc es en fi si ca co ne lm od el ad od ef en om en os fi si co sy as ip od er es tu di ar lo sy co mp re nd er lo sp od ri am os me nc io na rm uc ha sa re as do nd es ea pl ic al ac ar re ra qu eh an el eg id oy al go im po rt an te qu ed eb en pe ns ar en es te mo me nt oe sc ua ls er as us ig ui en te pa so