Criptografía y Seguridad
2019-2
Tarea 1

Profesor: Manuel Díaz Díaz

Alumnos:
Gladín García Ángel Iván
Martínez Ramos Gerardo Eugenio

1. Encontrar todas las las unidades de $\mathbb{Z}_{1024}$ y dada una unidad asociarla con su inverso multiplicativo.

(1,1)	(3,683)	(5,205)	(7,439)	(9,569)	(11,931)	(13,709)	(15,751)
(17,241)	(19,539)	(21,829)	(23,935)	(25,41)	(27,531)	(29,565)	(31,991)
(33,993)	(35,907)	(37,941)	(39,919)	(41,25)	(43,643)	(45,933)	(47,719)
(49,209)	(51,763)	(53,541)	(55,391)	(57,521)	(59,243)	(61,789)	(63,959)
(65,961)	(67,107)	(69,653)	(71,375)	(73,505)	(75,355)	(77,133)	(79,687)
(81,177)	(83,987)	(85,253)	(87,871)	(89,1001)	(91,979)	(93,1013)	(95,927)
(97,929)	(99,331)	(101,365)	(103,855)	(105,985)	(107,67)	(109,357)	(111,655)
(113,145)	(115,187)	(117,989)	(119,327)	(121,457)	(123,691)	(125,213)	(127,895)
(129,897)	(131,555)	(133,77)	(135,311)	(137,441)	(139,803)	(141,581)	(143,623)
(145,113)	(147,411)	(149,701)	(151,807)	(153,937)	(155,403)	(157,437)	(159,863)
(161,865)	(163,779)	(165,813)	(167,791)	(169,921)	(171,515)	(173,805)	(175,591)
(177,81)	(179,635)	(181,413)	(183,263)	(185,393)	(187,115)	(189,661)	(191,831)
(193,833)	(195,1003)	(197,525)	(199,247)	(201,377)	(203,227)	(205,5)	(207,559)
(209,49)	(211,859)	(213,125)	(215,743)	(217,873)	(219,851)	(221,885)	(223,799)
(225,801)	(227,203)	(229,237)	(231,727)	(233,857)	(235,963)	(237,229)	(239,527)
(241,17)	(243,59)	(245,861)	(247,199)	(249,329)	(251,563)	(253,85)	(255,767)
(257,769)	(259,427)	(261,973)	(263,183)	(265,313)	(267,675)	(269,453)	(271,495)
(273,1009)	(275,283)	(277,573)	(279,679)	(281,809)	(283,275)	(285,309)	(287,735)
(289,737)	(291,651)	(293,685)	(295,663)	(297,793)	(299,387)	(301,677)	(303,463)
(305,977)	(307,507)	(309,285)	(311,135)	(313,265)	(315,1011)	(317,533)	(319,703)
(321,705)	(323,875)	(325,397)	(327,119)	(329,249)	(331,99)	(333,901)	(335,431)
(337,945)	(339,731)	(341,1021)	(343,615)	(345,745)	(347,723)	(349,757)	(351,671)
(353,673)	(355,75)	(357,109)	(359,599)	(361,729)	(363,835)	(365,101)	(367,399)
(369,913)	(371,955)	(373,733)	(375,71)	(377,201)	(379,435)	(381,981)	(383,639)
(385,641)	(387,299)	(389,845)	(391,55)	(393,185)	(395,547)	(397,325)	(399,367)
(401,881)	(403,155)	(405,445)	(407,551)	(409,681)	(411,147)	(413,181)	(415,607)
(417,609)	(419,523)	(421,557)	(423,535)	(425,665)	(427,259)	(429,549)	(431,335)
(433,849)	(435,379)	(437,157)	(439,7)	(441,137)	(443,883)	(445,405)	(447,575)
(449,577)	(451,747)	(453,269)	(455,1015)	(457,121)	(459,995)	(461,773)	(463,303)
(465,817)	(467,603)	(469,893)	(471,487)	(473,617)	(475,595)	(477,629)	(479,543)
(481,545)	(483,971)	(485,1005)	(487,471)	(489,601)	(491,707)	(493,997)	(495,271)
(497,785)	(499,827)	(501,605)	(503,967)	(505,73)	(507,307)	(509,853)	(511,511)
(513,513)	(515,171)	(517,717)	(519,951)	(521,57)	(523,419)	(525,197)	(527,239)
(529,753)	(531,27)	(533,317)	(535,423)	(537,553)	(539,19)	(541,53)	(543,479)
(545,481)	(547,395)	(549,429)	(551,407)	(553,537)	(555,131)	(557,421)	(559,207)
(561,721)	(563,251)	(565,29)	(567,903)	(569,9)	(571,755)	(573,277)	(575,447)
(577,449)	(579,619)	(581,141)	(583,887)	(585,1017)	(587,867)	(589,645)	(591,175)
(593,689)	(595,475)	(597,765)	(599,359)	(601,489)	(603,467)	(605,501)	(607,415)
(609,417)	(611,843)	(613,877)	(615,343)	(617,473)	(619,579)	(621,869)	(623,143)
(625,657)	(627,699)	(629,477)	(631,839)	(633,969)	(635,179)	(637,725)	(639,383)
(641,385)	(643,43)	(645,589)	(647,823)	(649,953)	(651,291)	(653,69)	(655,111)
(657,625)	(659,923)	(661,189)	(663,295)	(665,425)	(667,915)	(669,949)	(671,351)
(673,353)	(675,267)	(677,301)	(679,279)	(681,409)	(683,3)	(685,293)	(687,79)
(689,593)	(691,123)	(693,925)	(695,775)	(697,905)	(699,627)	(701,149)	(703,319)
(705,321)	(707,491)	(709,13)	(711,759)	(713,889)	(715,739)	(717,517)	(719,47)
(721,561)	(723,347)	(725,637)	(727,231)	(729,361)	(731,339)	(733,373)	(735,287)
(737,289)	(739,715)	(741,749)	(743,215)	(745,345)	(747,451)	(749,741)	(751,15)
(753,529)	(755,571)	(757,349)	(759,711)	(761,841)	(763,51)	(765,597)	(767,255)
(769,257)	(771,939)	(773,461)	(775,695)	(777,825)	(779,163)	(781,965)	(783,1007)
(785,497)	(787,795)	(789,61)	(791,167)	(793,297)	(795,787)	(797,821)	(799,223)
(801,225)	(803,139)	(805,173)	(807,151)	(809,281)	(811,899)	(813,165)	(815,975)
(817,465)	(819,1019)	(821,797)	(823,647)	(825,777)	(827,499)	(829,21)	(831,191)
(833,193)	(835,363)	(837,909)	(839,631)	(841,761)	(843,611)	(845,389)	(847,943)
(849,433)	(851,219)	(853,509)	(855,103)	(857,233)	(859,211)	(861,245)	(863,159)
(865,161)	(867,587)	(869,621)	(871,87)	(873,217)	(875,323)	(877,613)	(879,911)
(881,401)	(883,443)	(885,221)	(887,583)	(889,713)	(891,947)	(893,469)	(895,127)
(897,129)	(899,811)	(901,333)	(903,567)	(905,697)	(907,35)	(909,837)	(911,879)
(913,369)	(915,667)	(917,957)	(919,39)	(921,169)	(923,659)	(925,693)	(927,95)
(929,97)	(931,11)	(933,45)	(935,23)	(937,153)	(939,771)	(941,37)	(943,847)
(945,337)	(947,891)	(949,669)	(951,519)	(953,649)	(955,371)	(957,917)	(959,63)
(961,65)	(963,235)	(965,781)	(967,503)	(969,633)	(971,483)	(973,261)	(975,815)
(977,305)	(979,91)	(981,381)	(983,999)	(985,105)	(987,83)	(989,117)	(991,31)
(993,33)	(995,459)	(997,493)	(999,983)	(1001,89)	(1003,195)	(1005,485)	(1007,783)
(1009,273)	(1011,315)	(1013,93)	(1015,455)	(1017,585)	(1019,819)	(1021,341)	(1023,1023)

Cuadro 1: Unidades y sus respectivos inversos en $\mathbb{Z}_{1024}$

Recordemos que $\overline{a}$ es una unidad en $\mathbb{Z}_n$ si y solo si $(a, n) = 1$

Entonces, para calcular las unidades y sus inversos se buscaron las combinaciones lineales de elementos en $\mathbb{Z}_{1024}$ tales que :

$$a(x) + 1024(y) = 1, \text{ donde } 0 < a < 1024$$

De esa forma se obtiene la unidad a y su inverso a^{-1} tal que $aa^{-1} \equiv 1 \pmod{1024}$

Por lo anterior y utilizando el siguiente código de Python se obtuvieron las 512 unidades de $\mathbb{Z}_{1024}$.

```
"""
Implementación del Algoritmo de Euclides Extendido
    Función que devuelve (g, x, y)
    donde a*x + b*y = g = mcd(a, b)
    a: entero
    b: entero
"""
def xmcd(a, b):
    x0, x1, y0, y1 = 0, 1, 1, 0
    while a != 0:
        q, b, a = b // a, a, b % a
        y0, y1 = y1, y0 - q * y1
        x0, x1 = x1, x0 - q * x1
    return b, x0, y0

"""
Función que calcula las unidades y sus inversos respecto a un módulo.
"""
def unidades(modulo):
    count = 0
    for i in range(0,modulo):
        g, x , y = xmcd(i,modulo)
        if g != 1 :
            continue
        else:
            aux = x
            if x < 0:
                aux = modulo + x
            print("("+str(i)+","+str(aux)+")")
            count += 1
    print("Se hallaron "+str(count)+" unidades.")
```

2. Resolver las siguientes congruencias y en caso de no tener solución decir por qué no tiene solución.

   a) $111x \equiv 75 \pmod{321}$

   Tiene solución porque $(111, 321) = 3$ y $3 \mid 75$ y por lo mismo podemos reducir el sistema al siguiente:

   $$37x \equiv 25 \pmod{107}$$

   Luego, utilizando el algoritmo extendido de Euclides vemos que $37(-26) + 107(9) = 1$
   por lo que -26 es el inverso de 37 (mód 107).
   $\Rightarrow (-26)37x \equiv (-26)25 \pmod{107}$
   $\Rightarrow x \equiv -650 \pmod{107}$
   $\Rightarrow x \equiv 99 \pmod{107}$
   $\therefore x = 99 + 107k$, $0 \leq k \leq 2$ son soluciones particulares y cualquier múltiplo de ellas también es solución.

b) $7x \equiv 5$ (mód 243)
Tiene solución porque $(7, 243) = 1$ y $1 \mid 243$
Luego, utilizando *AEE* vemos que $243(3) + 7(-104) = 1$
por lo que -104 es el inverso de 7 (mód 243), y $-104 \equiv 139$ (mód 243)
$\Rightarrow (139)7x \equiv (139)25$ (mód 243)
$\Rightarrow x \equiv 695$ (mód 243)
$\Rightarrow x \equiv 209$ (mód 243)
$\therefore x = 209 + 243k$, $k \in \mathbb{Z}$ es solución.

c) $15x \equiv 11$ (mód 625)
No tiene solución porque $(15, 625) = 5$ y $5 \nmid 11$

3. Resolver el siguiente sistema de ecuaciones usando el teorema chino del residuo.

$$x \equiv 32 \pmod{83} \quad (1)$$
$$x \equiv 70 \pmod{110} \quad (2)$$
$$x \equiv 30 \pmod{137} \quad (3)$$

Por el Teorema Chino del Residuo, el sistema tiene solución si y solo si

$(m_i, m_j) \mid (a_i - a_j)$, $\forall i, j \in \{1, ..., k\}$, m_k módulo y a_k miembro derecho de la congruencia.

- (1) y (2) tiene solución.
$$(83, 110) = 1 \mid 42 = (70 - 32)$$
- (1) y (3) tiene solución.
$$(83, 137) = 1 \mid 2 = (32 - 30)$$
- (2) y (3) tiene solución.
$$(110, 137) = 1 \mid 40 = (70 - 30)$$

Por lo anterior, el sistema (1), (2), (3) tiene solución. Primero resolvemos (1),(2):
$(1) \Rightarrow x = 32 + 83k_1$, $k_1 \in \mathbb{Z}$ ... (A)

Luego, sustituyendo la condición (A) en la congruencia (2):

$$(32 + 83k_1) \equiv 70 \pmod{110}$$
$$\Rightarrow 83k_1 \equiv 38 \pmod{110}, \text{ y por AEE: } 1 = 83(-53) + 110(40)$$
$$(-53)83k_1 \equiv (-53)70 \pmod{110}$$
$$-4399k_1 \equiv -3710 \pmod{110}$$
$$k_1 \equiv 76 \pmod{110}$$
$$\Rightarrow k_1 = 76 + 110k_2,\ k_2 \in \mathbb{Z} \text{ ...(B)}$$

Sustituyendo la condición (B) en la (A):

$$x = 32 + 83(76 + 110k_2)$$
$$\Rightarrow x = 6340 + 9130k_2$$
$$\therefore x \equiv 6340 \pmod{9130}, \text{ es solución de (1) y (2) ... (S1)}$$

Ahora, resolvemos el sistema (S1),(3):

$$(\text{S1}) \Rightarrow x = 6340 + 9130k_3,\ k_3 \in \mathbb{Z} \text{ ... (C)}$$

Sustituyendo (C) en (3):

$$6340 + 9130k_3 \equiv 30 \text{ (mód 137)}$$

$$9130k_3 \equiv -6310 \text{ (mód 137)}$$

$$88k_3 \equiv 129 \text{ (mód 137)},\text{y por AEE } 1 = 88(-14) + 9(137)$$

$$(-14)88k_3 \equiv (-14)129 \text{ (mód 137)}$$

$$-1232k_3 \equiv -1806 \text{ (mód 137)}$$

$$k_3 \equiv 112 \text{ (mód 137)}$$

$$\Rightarrow k_3 = 112 + 137k_4,\ k_4 \in \mathbb{Z} \ldots(\text{D})$$

Sustituyendo (D) en (C):

$$x = 6340 + 9130(112 + 137k_4),\ k_4 \in \mathbb{Z}$$

$$x = 1028990 + 1250810k_4$$

$$\therefore x \equiv 1028900 \text{ (mód 1250810) es la solución del sistema (1),(2),(3)}$$

4. Descifrar el siguiente mensaje el cual se sabe que está cifrado con un sistema monoalfabético y dar la clave en caso de haberla.

```
EMOHARH RGKTNOM OQMJKRFFOM EOP AREMOHARH QTGTFQJ ER ARHQR BTFFO HJ COY
RH OFRGOH RLTIUOFRHQR RXOSQJ ER FO GTSCRETGBMR PR EISR RIHR GRHAR FRTQR THO
SOHQIEOE ER ARHQR.
ERM FOERH FO QIRHEO EOP WOMRHCOTP TH AMOH OFGOSRH QIRHEO EJHER COY ER QJEJ
EIR WOMR FO GRMSOHSIO.
KFOHFJP PIH KFOH OF OZOM.
CRMTGIMMRH OHEOM KJM TH FOEJ Y KJM JQMJ.
WOP PQRCQ ZT EIRHPQRH J WJ GIQ DOHH ISC EIRHRH PJH VJMGTFOP SJMMIRHQRP KOMO
ERSIM RH LTR FR KTREJ PRMUIM O TPQRE LTR GOHEO TPQRE.
EIR QMOTRM RF FTQJ.
EIR OBQRIFTHA FO PRSSIJH RF ERKOMQOGRHQJ.
```

Lo primero que hay que hacer es obtener la tabla de frecuencias, para esto nos apoyamos con un programa para calcularlas.

```python
def frecuencias(archivo):
    f = open(archivo,'r')
    text = f.readlines()
    # Asignamos un lista que tendrá tres valores
    # El primero la letra correspondiente, la frecuencia
    # y porcentaje, respectivamente.
    l = [[chr(65+i), 0, ''] for i in range(26)]
    tot = 0
    for line in text:
        for char in line:
            if (char == ' ' or char == '\n' or char == '.'):
                continue
            else:
                l[ord(char)-65][1] += 1
                tot+=1

    for i in range(len(l)):
        # Obtenemos el porcentaje.
```

```
        l[i][2] = (l[i][1]*100) / tot
        l[i][2]= format(l[i][2], '.2f')

    #Ordenamos con respecto a la frecuencia.
    l.sort(key=lambda x: x[1], reverse=True)

    return l
```

Dando de resultado lo siguiente:

Letra	Frec	%	Letra	Frec.	%
R	66	15.60	K	9	2.13
O	52	12.29	A	8	1.89
H	42	9.93	C	7	1.65
E	32	7.57	W	4	0.95
M	29	6.86	B	3	0.71
F	25	5.91	L	3	0.71
Q	25	5.91	Y	3	0.71
T	23	5.44	U	2	0.47
J	22	5.20	Z	2	0.47
I	21	4.96	D	1	0.24
P	16	3.78	N	1	0.24
G	13	3.07	V	1	0.24
S	12	2.84	X	1	0.24

Cuadro 2: Tabla de frecuencias de los sçimbolos en el texto cifrado

Lo primero a notar es que fue cifrada con un sistema monoalfabético, lo cual podemos intentar con dezplazamientos (como Caesar), diezmado o afín. No tuvimos éxito con esos así que se decidió analizar por frecuencias. Usando la frecuenacias[1], tenemos que en nuestrá tabla de frecuencis la `R` podría ser candidato a ser `e` porque la `e` la distribución de la letra es la más alta (13.06). Luego viendo de nuevo la tabla del Apéndice A, suponiendo que el texto estaría en español tenemos a `RF`[2] que si sustituimos $[R := e]$ se tiene que `eF` y si probamos como candidato a `F` como `l` se tiene que `el`. Seleccionamos la el porque igual en la tabla de frecuencias `el` es una palabra muy utilizada en español. Ahora tenemos lo siguiente:

```
EMOHAeH eGKTNOM OQMJKellOM EOP AeEMOHAeH QTGTlQJ Ee AeHQe BTllO HJ COY
EMOHARH RGKTNOM OQMJKRFFOM EOP AREMOHARH QTGTFQJ ER ARHQR BTFFO HJ COY

eH OleGOH eLTIUOleHQe eXOSQJ Ee lO GTSCeETGBMe Pe EISe eIHe GeHAe leTQe THO
RH OFRGOH RLTIUOFRHQR RXOSQJ ER FO GTSCRETGBMR PR EISR RIHR GRHAR FRTQR THO

SOHQIEOE Ee AeHQe.
SOHQIEOE ER ARHQR.

EeM lOEeH lO QIeHEO EOP WOMeHCOTP TH AMOH OlGOSeH QIeHEO EJHEe COY Ee QJEJ
ERM FOERH FO QIRHEO EOP WOMRHCOTP TH AMOH OFGOSRH QIRHEO EJHER COY ER QJEJ
```

[1] Del apéndice A del libro de Criptografía de Galaviz
[2] La tercera pabalabra del penúltimo renglón

```
EIe WOMe lO GeMSOHSIO.
EIR WOMR FO GRMSOHSIO.

KlOHlJP PIH KlOH Ol OZOM.
KFOHFJP PIH KFOH OF OZOM.

CeMTGIMMeH OHEOM KJM TH lOEJ Y KJM JQMJ.
CRMTGIMMRH OHEOM KJM TH FOEJ Y KJM JQMJ.

WOP PQeCQ ZT EIeHPQeH J WJ GIQ DOHH ISC EIeHeH PJH VJMGTlOP SJMMIeHQeP KOMO
WOP PQRCQ ZT EIRHPQRH J WJ GIQ DOHH ISC EIRHRH PJH VJMGTFOP SJMMIRHQRP KOMO

EeSIM eH LTe le KTeEJ PeMUIM O TPQeE LTe GOHEO TPQeE.
ERSIM RH LTR FR KTREJ PRMUIM O TPQRE LTR GOHEO TPQRE.

EIe QMOTeM el lTQJ.
EIR QMOTRM RF FTQJ.

EIe OBQeIlTHA lO PeSSIJH el EeKOMQOGeHQJ.
EIR OBQRIFTHA FO PRSSIJH RF ERKOMQOGRHQJ.
```

Analizando de nuevo las frecuencias, podríamos intentar haciendo la sustitución de $[H := n]$. Haciendo esto vemos la apración de la preposición `en` dos veces, lo cual nos indica que igual es un buen candidato. Analizando de nuevo la tabla de frecuencias, encontramos tres veces `LT` seguidos de una `e` y una I, lo cual nos da el indición de que el mejor candidato podrías ser la `qu` y así cumple porque depués es precesdido por una e y también supondríamos que $[I := i]$, así formando `que` y qui. También tomando como única palabra de una letra la `Y` como `y`. Así dando como reslutado que $[Y := y]$, $[I := i]$, $[L := q]$ y $[T := u]$. Con las sustituciones así se vería el texto hasta ahora.

```
EMOnAen eGKuNOM OQMJKellOM EOP AeEMOnAen QuGulQJ Ee AenQe BullO nJ COy
EMOHARH RGKTNOM OQMJKRFFOM EOP AREMOHARH QTGTFQJ ER ARHQR BTFFO HJ COY

en OleGOn equIUOlenQe eXOSQJ Ee lO GuSCeEuGBMe Pe EISe eIne GenAe leuQe unO
RH OFRGOH RLTIUOFRHQR RXOSQJ ER FO GTSCRETGBMR PR EISR RIHR GRHAR FRTQR THO

SOnQIEOE Ee AenQe.
SOHQIEOE ER ARHQR.

EeM lOEen lO QIenEO EOP WOMenCOuP un AMOn OlGOSen QIenEO EJnEe COy Ee QJEJ
ERM FOERH FO QIRHEO EOP WOMRHCOTP TH AMOH OFGOSRH QIRHEO EJHER COY ER QJEJ

EIe WOMe lO GeMSOnSIO.
EIR WOMR FO GRMSOHSIO.

KlOnlJP PIn KlOn Ol OZOM.
KFOHFJP PIH KFOH OF OZOM.

CeMuGIMMen OnEOM KJM un lOEJ y KJM JQMJ.
CRMTGIMMRH OHEOM KJM TH FOEJ Y KJM JQMJ.

WOP PQeCQ Zu EIenPQen J WJ GIQ DOnn ISC EIenen PJn VJMGulOP SJMMIenQeP KOMO
WOP PQRCQ ZT EIRHPQRH J WJ GIQ DOHH ISC EIRHRH PJH VJMGTFOP SJMMIRHQRP KOMO
```

```
EeSIM en que le KueEJ PeMUIM O uPQeE que GOnEO uPQeE.
ERSIM RH LTR FR KTREJ PRMUIM O TPQRE LTR GOHEO TPQRE.

EIe QMOueM el luQJ.
EIR QMOTRM RF FTQJ.

EIe OBQeIlunA lO PeSSIJn el EeKOMQOGenQJ.
EIR OBQRIFTHA FO PRSSIJH RF ERKOMQOGRHQJ.
```

Hata este punto sabemos que vamos bien porquw encotramos algo que tiene sentido `en que le` en el tercer renglón (de abajo hacia arriba), igual mirando la tabla de frencuacias y a prueba y errores, se cree que sería un buen candidato $[E := d]$, $[S := c]$, $[M := r]$. Suponemos que `O` es la `a` porque la `a` y `e` son las letras con mayor frecuancia en español así que tomamos $[O := a]$. Hasta este punto el texto empeza a tener sentido la parte de `decir en que le KuedJ PerUir a uPQed que Ganda uPQed.`, de nuevo bajo la misma lógica se sustituirá, $[K := p]$, $[J := o]$, $[P := s]$, $[Q := t]$, $[V := f]$, $[G := m]$, $[U := v]$, $[N := j]$, $[A := g]$, $[U := v]$, $[C := h]$ Entonces hasta este punto tenemos que:

```
drangen empujar atropellar das gedrangen tumulto de gente Bulla no hay
EMOHARH RGKTNOM OQMJKRFFOM EOP AREMOHARH QTGTFQJ ER ARHQR BTFFO HJ COY

en aleman equivalente eXacto de la muchedumBre se dice eine menge leute una
RH OFRGOH RLTIUOFRHQR RXOSQJ ER FO GTSCRETGBMR PR EISR RIHR GRHAR FRTQR THO

cantidad de gente.
SOHQIEOE ER ARHQR.

der laden la tienda das Warenhaus un gran almacen tienda donde hay de todo
ERM FOERH FO QIRHEO EOP WOMRHCOTP TH AMOH OFGOSRH QIRHEO EJHER COY ER QJEJ

die Ware la mercancia.
EIR WOMR FO GRMSOHSIO.

planlos sin plan al aZar.
KFOHFJP PIH KFOH OF OZOM.

herumirren andar por un lado y por otro.
CRMTGIMMRH OHEOM KJM TH FOEJ Y KJM JQMJ.

Was steht Zu diensten o Wo mit Dann ich dienen son formulas corrientes para
WOP PQRCQ ZT EIRHPQRH J WJ GIQ DOHH ISC EIRHRH PJH VJMGTFOP SJMMIRHQRP KOMO

decir en que le puedo servir a usted que manda usted.
ERSIM RH LTR FR KTREJ PRMUIM O TPQRE LTR GOHEO TPQRE.

die trauer el luto.
EIR QMOTRM RF FTQJ.

die aBteilung la seccion el departamento.
EIR OBQRIFTHA FO PRSSIJH RF ERKOMQOGRHQJ.
```

Notamos también que hay precencia de alemán(?), por lo que haremos el mapeo para ver si nos puede dar una pista

- A $\longrightarrow$ o
- B $\longrightarrow$ b
- C $\longrightarrow$ s
- D $\longrightarrow$ e
- E $\longrightarrow$ r
- F $\longrightarrow$ v
- G $\longrightarrow$ a
- H $\longrightarrow$ c
- I $\longrightarrow$ i
- J $\longrightarrow$?
- K $\longrightarrow$?
- L $\longrightarrow$?
- M $\longrightarrow$?
- N $\longrightarrow$ h
- O $\longrightarrow$ j
- P $\longrightarrow$ k
- Q $\longrightarrow$ l
- R $\longrightarrow$ m
- S $\longrightarrow$ p
- T $\longrightarrow$ q
- U $\longrightarrow$ t
- V $\longrightarrow$?
- W $\longrightarrow$?
- X $\longrightarrow$?
- Y $\longrightarrow$ y
- Z $\longrightarrow$?

De esta forma ya parece un algo intuitivo llenar los demás espacios.

- A $\longrightarrow$ o
- B $\longrightarrow$ b
- C $\longrightarrow$ s
- D $\longrightarrow$ e
- E $\longrightarrow$ r
- F $\longrightarrow$ v
- G $\longrightarrow$ a
- H $\longrightarrow$ c
- I $\longrightarrow$ i
- J $\longrightarrow$ n
- K $\longrightarrow$ d
- L $\longrightarrow$ f
- M $\longrightarrow$ g
- N $\longrightarrow$ h

- O $\longrightarrow$ j
- P $\longrightarrow$ k
- Q $\longrightarrow$ l
- R $\longrightarrow$ m
- S $\longrightarrow$ p
- T $\longrightarrow$ q
- U $\longrightarrow$ t
- V $\longrightarrow$ u
- W $\longrightarrow$ w
- X $\longrightarrow$ x
- Y $\longrightarrow$ y
- Z $\longrightarrow$ z

Habiendo hecho este análisis se sigue que, (por algo visto en clase), que la palabra clave sería `observacion`, digo visto en clase porque si quitarmos caracteres repetidos es `observacin`.
Dando como resultado que la secuencia de letras queda de la forma.

$$OBSERVACINDFGHJKLMPQTUWXYZ$$

Con un script para descifrar el mensaje el cual es:

```
alf = ['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']
key = ['O', 'B', 'S', 'E', 'R', 'V', 'A', 'C', 'I', 'N', 'D', 'F', 'G',
       'H', 'J', 'K', 'L', 'M', 'P', 'Q', 'T', 'U', 'W', 'X', 'Y', 'Z']

f = dict()
for i in range(26):
    f[key[i]] = alf[i]

def descifra(archivo):
    file = open(archivo,'r')
    text = file.readlines()
    r = ''
    for line in text:
        for char in line:
            if char.isalpha():
                print(f[char], end='')
            else:
                print(char, end='')

descifra('ej4.txt')
```

Dando como resultado el siguiente texto.

```
DRANGEN EMPUJAR ATROPELLAR DAS GEDRANGEN TUMULTO DE GENTE BULLA NO HAY
EN ALEMAN EQUIVALENTE EXACTO DE LA MUCHEDUMBRE SE DICE EINE MENGE LEUTE UNA
CANTIDAD DE GENTE.
DER LADEN LA TIENDA DAS WARENHAUS UN GRAN ALMACEN TIENDA DONDE HAY DE TODO
DIE WARE LA MERCANCIA.
PLANLOS SIN PLAN AL AZAR.
HERUMIRREN ANDAR POR UN LADO Y POR OTRO.
```

```
WAS STEHT ZU DIENSTEN O WO MIT KANN ICH DIENEN SON FORMULAS CORRIENTES PARA
DECIR EN QUE LE PUEDO SERVIR A USTED QUE MANDA USTED.
DIE TRAUER EL LUTO.
DIE ABTEILUNG LA SECCION EL DEPARTAMENTO.
```

5. Descifrar el mensaje que fue encriptado con Vigenère, recuerda que debes encontrar la longitud y la clave usando índices de coincidencias.

```
FUDPBVEQAH KEYECSUQWS KMBPFVIPDQ NAETSPLMUO EUXIOFDQRW
GNOXOUHQCC VAPDEWEQCZ QSXXPTOESS EAXRINOBPF VEZSSSUQTZ
EOZYIPTASS NOECIOEDDG TEMASUEEJB EAYECAJMBO UDQBIGSFGO
PQGTZQEEEC TLAFIGSAAC GXTXPGNEJG RRAEWGDMSS UYVPACSPTA
WEEIFCNCJS NOETGAACJS POQHHCNETB EIXACRODFI GHMNEWEODB
UTDJWTEXRO OPASSNOECI OEDDGTEMAS UYQHCKMBAW EAYPBGJMGS
NCACQGPFDR GSGRSUIACS UDQROWCTNJ GAYDGGNFDB EEEFIGCABS
PTMCZQSMJH QRQHHQMYPD QSFDZASBXJ CCQAGKSFTA COOPAROPTZ
QSZJAGRAHF GAXTGGSGCC FEXDGEOZRS RTAHTWNPPA GNFPZGSPTZ
CMMISOAFXQ CUZTGVUPXC TISJFQSANS ZHMJGVIHDR GLMCONIEXG
OAFTACTURC TECJSTIDXO NAUCQNUEXC PDQJBCDQUW PIOXCPCGXR
CDAHOFEXHW INUUWEAPDR GLZJAGRAGS CLGCOFIERI UIACFGLMIW
XAMAOEOZHH TUORWQNPTZ QSZJAGRAHF GAXTGAUZPS ZPAHWEIACR
GSUHDTIZRW RAXTGRRAEW GDMSSUSUQW GNQHHCSZDQ KOZTGDAEXQ
CSODBUTUII AEZJBCPMGH GMGNWPTQGS UAZISFEXDG HUZSOOEZIC
UDQAOUMMIS OAFXQCSZDG GRMCHTAFPR CSMFIKCACR GTMAZGEZGS
CLUSOFEZAO OAKDFKAPTZ CSRPGGSPTZ CNMAWUIEBO UQGTZQSYTH
QDAHIUAPDG GNXPQQNEIF WCOXCPDQAQ CMBDRGLAHB WMQGCURQPZ
GSZDGKNFTF GSMCGWSBGC RIQSOFEEEC TLAIOPTAIC OADTAQSGCD
GQGTBQGDJD QDQPLKOYPG FEXDGEUMAS UPGTRGNPTR WCUGGGTASO
ULMHDTOBXS FAPTGFEXDG PUYTFQSDTO NEEEOTAMWC PDMGSPLAHA
GTASCUUFXZ KZMSCUEZAO EOZHHTUORW QNPTZEAYEC TEMASNLQRH
QRPTPGRUPQ QNEJZVADAO URQUSTEZRW CSNXPNIAVF CFUROUDQAT
KNMARGLOPD KTGACGLFXH WLASSGSFTQ CPUIINOQMD TEEPSPPARO
UPMAODRMHZ QSODBQCUBW GNFDGOAFTA CTURCUNQRS UADXCUPMGO
NEQGSUTQAW DRASSJEOWC GSFTQQRFDQ CPUIINOQHG KMBASOEZIS
WNMTLRLURO EIACRGLAFI GSQTBVIQCR GPAGDTOBXS FAPTGDAEXQ
CSPTZQSZJA GRAHHQDMHZ CSOJONEEHI OAKBINTUEZ KCMRWQNDTG
VAKSWXIEXC PRQHCNUOXC PDQTQWAOXC PEEUOETAGW BAOXCPYAIF
QSBGCEEEDG CLSTPTAURC UNAHGQNKPQ QNARWFAEHW PEYQOTGATG
VEOPDKTGAC POQHIPRQEO UOMESUADSS NOODBQCUSC FEXPACTQGW
CLMTLRLAGO EIACEWEHPA QSMTARRQCR GRQHDTONPP NECJSRADTN
EAZDJGDMSB QSQIFCTMSS RRQHSPTMGI PADTJKSUDB RRAAWLAPTA
CTQGWCSFGO FIOXCPAXTG UIZDRGSUCH GRUOOTEEIS XIQYCUANTF
GNGCFGDGRW FOPTDTOBXS FAPTGUEZRW NLMHDCRMHS TMQCQKOZPR
CSBTFQVMPF GSGAHCRCJS WNEDFRRQCR GNFTBWMQGC FEPXJGREDG
JEOWCUIYEC TTMCHGSETC DTQCRTAODA QCACGGCGTB EIMSSNAEFI
GVMBCUAPTG VAOPFFEXPG FOOTDTOBXS FAPTGSUQKO OOEPSUTGSW
CRQCSUTQRO RIFJZQLMHB WEHTDTIYTF CSETFGFUTF GNMAOUOBTF
CCUDBGSRJB FAYTBVAXTG FEEJACYYJZ VIBAWEAOXC PATDFCVQPA
QSXDEWEPXQ GPUHYWNAKI POPTZQSODB EEBICUFGCR CMQCHCLQHR
GLMHACTQBO VIOPGGSQAB WMQGCGLODB EEBICFEZJA GRAHITGUDS
PLMPBVISJS FAPPARLUPB FOETMIEZTF CLUOOPDAHS EOZTZVIQBD
QLAHBWMQGC UEZISTOEIT TAORWQNQHG GLXPACNZJA GRAHFCCUDB
CLQHSNNGBS TODPQKOZPZ RUQSSGXBDB GRETQQMAAO TALDBFEXDG
PUYTFQSQCH GRAHDAQFPZ GSCJSRYCHC PPDXAQSDTZ CTUKCUEEIC
UNGBSTOEEI GDQCFGPDTG GNFPFUEBDF HRMRQKOZTG REDXCFIOPG
HIZXHCSAXB HIZXHCSXDG PUYTFQSCJS POFXSPEZJB CEJEOUIACR
GCUBONCURZ KCMHSNEEAZ CMMXFTAOXC PAXTGGLODB LUZICSUQGS
UUXIOFEXPI PIACRGLAHF CCUDBCLQHQ QNXDGKRDPQ KOZPZGSETZ
GLXPACCACX WNFDRGLAHB WMQGCURQPZ GSQCSUTMEO TTQTJCDQTZ
CUFDFVOOPF GLBJBVOPDB FEETQQNEIF WYQCZQSZJA GRAHFGAXTG
NAODBELGHW QNQHEWEZXB IUZAWDRASS EAXRINOXDH TAFPFCPGTG
GSHTFFAPHC NOZDGKMBDF VAXPQQMBAS VELSSNOECI OEDDGTEMAS
UPMGOCSQVI TADFIGEJXG VAZACULUBW VEE
```

Lo primero que hay que hacer es buscar patrones repetidos, una vez teniendo eso podremos analizar la secuencia, posición, distancia y factores. Para esto haremos un programa que nos ayude con dicha tarea. Ahora bien, se hizo un script en Python para encontrar patrones repetidos y así facilitarnos la tarea, como se nos dio la pequeña pista de que la clave era al menos de longitud cinco decidimos buscar coincidencias de esa longitud y sus múltiplos. Teniendo en cuenta eso, se mostrará el programa para encontrar las apariciones:

```
s = 'FUDPBVEQAHKEYECSUQWSKMBPFVIPDQNAETSPLMUOEUXIOFDQRWGNOXOUHQCCVAPDEWEQCZQSXXPTOESSEAXRINOBPFVEZS

def parse_pos_a_distancias(l):
    s = ''
    ln = len(l)
    for i in range(ln - 1):
        n = l[i + 1] - l[i]
        s += str(n)
        if i < ln - 2:
```

```
            s += ', '
    return s

start = 5
end = 20
l = len(s)

d = dict()
for i in range(start, end):
    for k in range(l - i):
        aux = s[k:k + i]
        if aux not in d:
            d[aux] = [k]
        else:
            d[aux].append(k)

for (k, v,) in d.items():
    if len(k) % 5 == 0 and len(v) > 3:
        print('secuencia: {}, longitud: {}, posicion: {}, distancia: {}, factores:'.format(
            k, len(k), ','.join(map(str, v)), parse_pos_a_distancias(v)))
```

Dandonos como resultado esto:

```
secuencia: TEMAS, longitud: 5, posicion: 120,275,1090,2695, distancia: 155, 815, 1605, factores:
secuencia: PTZQS, longitud: 5, posicion: 397,617,1352,2022, distancia: 220, 735, 670, factores:
secuencia: ZQSZJ, longitud: 5, posicion: 399,619,1354,2584, distancia: 220, 735, 1230, factores:
secuencia: QSZJA, longitud: 5, posicion: 400,620,1355,2585, distancia: 220, 735, 1230, factores:
secuencia: SZJAG, longitud: 5, posicion: 401,621,1356,2586, distancia: 220, 735, 1230, factores:
secuencia: ZJAGR, longitud: 5, posicion: 402,572,622,1357,2087,2187,2587, distancia: 170, 50, 735, 730, 100, 4
secuencia: JAGRA, longitud: 5, posicion: 403,573,623,1358,2088,2188,2588, distancia: 170, 50, 735, 730, 100, 4
secuencia: AGRAH, longitud: 5, posicion: 404,624,1359,2089,2189,2589, distancia: 220, 735, 730, 100, 400, fact
secuencia: GRAHF, longitud: 5, posicion: 405,625,2190,2590, distancia: 220, 1565, 400, factores:
secuencia: FEXDG, longitud: 5, posicion: 420,735,970,1015,2245, distancia: 315, 235, 45, 1230, factores:
secuencia: IACRG, longitud: 5, posicion: 646,1311,2396,2461, distancia: 665, 1085, 65, factores:
secuencia: BWMQG, longitud: 5, posicion: 889,1784,2069,2154,2519, distancia: 895, 285, 85, 365, factores:
secuencia: WMQGC, longitud: 5, posicion: 890,1785,2070,2155,2520, distancia: 895, 285, 85, 365, factores:
secuencia: DTOBX, longitud: 5, posicion: 1004,1334,1714,1874, distancia: 330, 380, 160, factores:
secuencia: TOBXS, longitud: 5, posicion: 1005,1335,1715,1875, distancia: 330, 380, 160, factores:
secuencia: OBXSF, longitud: 5, posicion: 1006,1336,1716,1876, distancia: 330, 380, 160, factores:
secuencia: BXSFA, longitud: 5, posicion: 1007,1337,1717,1877, distancia: 330, 380, 160, factores:
secuencia: XSFAP, longitud: 5, posicion: 1008,1338,1718,1878, distancia: 330, 380, 160, factores:
secuencia: SFAPT, longitud: 5, posicion: 1009,1339,1719,1879, distancia: 330, 380, 160, factores:
secuencia: FAPTG, longitud: 5, posicion: 1010,1340,1720,1880, distancia: 330, 380, 160, factores:
secuencia: AOXCP, longitud: 5, posicion: 1426,1441,1986,2426, distancia: 15, 545, 440, factores:
secuencia: ZQSZJAGRAH, longitud: 10, posicion: 399,619,1354,2584, distancia: 220, 735, 1230, factores:
secuencia: DTOBXSFAPT, longitud: 10, posicion: 1004,1334,1714,1874, distancia: 330, 380, 160, factores:
secuencia: TOBXSFAPTG, longitud: 10, posicion: 1005,1335,1715,1875, distancia: 330, 380, 160, factores:
```

Y como son módulo cinco su descomposición en primos es de la forma $n = 5$ o $n = 5 \cdot 2$. Teniendo esto en mente, y analizando **exhaustivamente**[3] a las frecuencias en las columnas, dimos con la clave.

Después de todo este análisis notamos que la clave es:

$$CAMPO$$

Programa para descifrar el texto e imprimirlo en terminal.

[3]Después de dos frustantes días haciendo intento tras intento en hojas de papel, analizando los posibles casos, rayando muchas hojas sin llegar a nada por horas, y viendo el ejercicio hecho en clase y las notas de Galaviz.

```
llave = 'CAMPO'

def descifra_vigener(x, k):
    n1 = ord(x)-65
    n2 = ord(k)-65
    return (n1-n2)%26

def descifra(archivo):
    file = open(archivo,'r')
    text = file.readlines()
    r = ''
    i = 0
    for line in text:
        for char in line:
            if char.isalpha():
                c = llave[i%len(llave)]
                r = chr(descifra_vigener(char, c)+65)
                print(r, end='')
                i += 1
            else:
                print(char, end='')

descifra('ej5.txt')
```

Lo que da como resultado:

```
DURANTEELT IEMPOQUEHE IMPARTIDOC LASEENLAFA CULTADDECI
ENCIASHENO TADOQUEENL OSLIBROSDE CALCULOPAR TENDEQUEEL
CONJUNTODE LOSNUMEROS REALESESUN CAMPOYJAMA SDEMUESTRA
NQUELOESPO RLOQUESOLO EXHIBENSUS PROPIEDADE SYJAMASDEM
UESTRANQUE LOSESYAQUE NOESTANSEN CILLOPORQU EHAYQUECON
STRUIRELCA MPODELOSNU MEROSREALE SYESOIMPLI CAMANEJARE
LCONCEPTOD ESUCESIONE SDECAUCHYV EAMOSENTON CESQUECOME
NTANLOSAUT ORESTOMMAP OSTOLYSPIV ACELSISTEM AOCAMPODEL
OSNUMEROSR EALESESUNO DELOSCONCE PTOSFUNDAM ENTALESDEL
AMATEMATIC AUNESTUDIO RIGUROSOYE XHAUSTIVOD ELANALISIS
MATEMATICO REQUERIRIA LAINCLUSIO NDEUNADEFI NICIONCUID
ADOSADELSI GNIFICADOD ELNUMERORE ALUNADISCU SIONRELATI
VAALACONST RUCCIONDEL OSNUMEROSR EALESYUNAE XPOSICIOND
ESISPRINCI PALESPROPI EDADESSIBI ENESTASNOC IONESBASIC
ASCONSTITU YENUNAPART EMUYINTERE SANTEDELOS FUNDAMENTO
SDELASMATE MATICASNOS ERANTRATAD ASAQUICOND ETALLEENRE
ALIDADENLA MAYORIADEL ASFASESDEL ANALISISMA SQUELOSMET
ODOSUSADOS ENLACONSTR UCCIONDELC AMPODELOSN UMEROSREAL
ESNOSINTER ESANSUSPRO PIEDADESPO RLOTANTOTO MAREMOSUNP
EQUENOGRUP ODEAXIOMAS DELOSCUALE SPUEDENDED UCIRSETODA
SLASPROPIE DADESDELOS NUMEROSREA LESPARAAHO NDARENLOSM
ETODOSUTIL IZADOSENLA CONSTRUCCI ONDELCAMPO REALELLECT
ORDEBERIAC ONSULTARLA SREFERENCI ASBIBLIOGR AFICASDELF
INALDELCAP ITULOELTIT ULODEESTEC APITULOEXP RESAENPOCA
SPALABRASL OSCONOCIMI ENTOSMATEM ATICOSNECE SARIOSPARA
LEERESTELI BRODEHECHO ESTECORTOC APITULOESS IMPLEMENTE
UNAEXPLICA CIONDELOQU ESEENTIEND EPORPROPIE DADESBASIC
ASDELOSNUM EROSTODASL ASCUALESSU MAYMULTIPL ICACIONRES
TAYDIVISIO NRESOLUCIO NDEECUACIO NESFACTORI ZACIONYOTR
OSPROCESOS ALGEBRAICO SNOSSONYAC ONOCIDASSI NEMBARGOES
TECAPITULO NOESUNREPA SOAPESARDE LOCONOCIDO DELAMATERI
ALAEXPLORA CIONQUEVAM OSAEMPREND ERESPROBAB LEQUEPAREZ
```

```
CANOVEDADN OSETRATADE PRESENTARU NAREVISION PROLIJADEM
ATERIASTRA DICIONALES SINODESINT ERIZARESTE VIEJOSABER
ENUNREDUCI DODEPROPIE DADESSENCI LLASPARASE RMENCIONAD
ASPEROVAAR ESULTARQUE UNSORPREND ENTENUMERO DEDIVERSOS
HECHOSIMPO RTANTESSEO BTENDRACOM OCONSECUEN CIADELASQU
EVAMOSADES TACARDELAS DOCEPROPIE DADESQUEVA MOSAESTUDI
ARENESTECA PITULOLASN UEVEPRIMER ASSEREFIER ENALASOPER
ACIONESFUN DAMENTALES DESUMAYMUL TIPLICACIO NAHORAVEAM
OSLOQUEDIC EPISKUNOVU NODELOSCON CEPTOSFUND AMENTALESD
ELASMATEMA TICASESELN UMEROELCON CEPTODENUM EROSURGIOE
NLAANTIGUE DADAMPLIAN DOSEYGENER ALIZANDOSE CONELTIEMP
OLOSNUMERO SENTEROSTF RACCIONESS ELLAMANNUM EROSRACION
ALESELNUME RORACIONAL PUEDEEXPON ERSECOMOLA RAZONDELOS
NUMEROSENT EROSPYQTAL ESQUEPYQSO NPRIMOSREL ATIVOSESTO
SNUMEROSPU EDENREPRES ENTARSEPOR FRACCIONES PERIODICAS
FINITASOIN FINITASLOS NUMEROSQUE NOTIENENUN AEXPASIOND
ECIMALCICL ICASELESLL AMAIRRACIO NALESELCON JUNTOQUERE
SULTADELAU NIONDELOSR ACIONALESC ONLOSIRRAC IONALESSEL
ELLAMACONJ UNTODELOSN UMEROSREAL ESENESTAPA RTEEVADEEL
AUTORTOCAR ELPUNTODON DESECONSTR UYENLOSNUM EROSREALES
LACONCLUSI ONESQUENIN GUNLIBRODE CALCULOLOT RATARAPUES
ESVERDADSO LONOSIMPOR TALACOMPLE TEZDELOSNU MEROSREALE
SPARAASEGU RARQUEEXIS TANLOSLIMI TES
```

Y dando una separación adecuada se tiene:

```
DURANTE EL TIEMPO QUE HE IMPARTIDO CLASE EN LA FACULTAD DE CIENCIAS HE NOTADO
QUE EN LOS LIBROS DE CALCULO PARTEN DE QUE EL CONJUNTO DE LOS NUMEROS REALES
ES UN CAMPO Y JAMAS DEMUESTRAN QUE LO ES POR LO QUE SOLO EXHIBEN SUS PROPIEDADES
Y JAMAS DEMUESTRAN QUE LOS ES YA QUE NO ES TAN SENCILLO PORQUE HAY QUE CONSTRUIR
EL CAMPO DE LOS NUMEROS REALES Y ESO IMPLICA MANEJAR EL CONCEPTO DE SUCESIONES
DE CAUCHY VEAMOS ENTONCES QUE COMENTAN LOS AUTORES TOMM APOSTOL Y SPIVAC EL
SISTEMA O CAMPO DE LOS NUMEROS REALES ES UNO DE LOS CONCEPTOS FUNDAMENTALES DEL
MATEMATICA UN ESTUDIO RIGUROSO Y EXHAUSTIVO DEL ANALISIS MATEMATICO REQUERIRIA
LA INCLUSION DE UNA DEFINICION CUIDADOSA DEL SIGNIFICADO DEL NUMERO REAL UNA
DISCUSION RELATIVA A LA CONSTRUCCION DE LOS NUMEROS REALES Y UNA EXPOSICION DE
SIS PRINCIPALES PROPIEDADES SI BIEN ESTAS NOCIONES BASICAS CONSTITUYEN UNA PARTE
MUY INTERESANTE DE LOS FUNDAMENTOS DE LAS MATEMATICAS NO SERAN TRATADAS AQUI CON
DETALLE EN REALIDAD EN LA MAYORIA DE LAS FASES DEL ANALISIS MAS QUE LOS METODOS
USADOS EN LA CONSTRUCCION DEL CAMPO DE LOS NUMEROS REALES NOS INTERESAN SUS
PROPIEDADES POR LO TANTO TOMAREMOS UN PEQUENO GRUPO DE AXIOMAS DE LOS CUALES
PUEDEN DEDUCIRSE TODAS LAS PROPIEDADES DE LOS NUMEROS REALES PARA AHONDAR EN LOS
METODOS UTILIZADOS EN LA CONSTRUCCION DEL CAMPO REAL EL LECTOR DEBERIA
CONSULTARLAS REFERENCIAS BIBLIOGRAFICAS DEL FINAL DEL CAPITULO EL TITULO DE ESTE
CAPITULO EXPRESA EN POCAS PALABRAS LOS CONOCIMIENTOS MATEMATICOS NECESARIOS PARA
LEER ESTE LIBRO DE HECHO ESTE CORTO CAPITULO ES SIMPLEMENTE UNA EXPLICACION DE LO
QUE SE ENTIENDE POR PROPIEDADES BASICAS DE LOS NUMEROS TODAS LAS CUALES SUMA Y
MULTIPLICACION RESTA Y DIVISION RESOLUCION DE ECUACIONES FACTORIZACION Y OTROS
PROCESOS ALGEBRAICOS NOS SON YA CONOCIDAS SIN EMBARGO ESTE CAPITULO NO ES UN
REPASO A PESAR DE LO CONOCIDO DE LA MATERIA LA EXPLORACION QUE VAMOS A EMPRENDER
ES PROBABLE QUE PAREZCA NOVEDAD NO SE TRATA DE PRESENTAR UNA REVISION PROLIJA
DE MATERIAS TRADICIONALES SI NO DE SINTERIZAR ESTE VIEJO SABER EN UN REDUCIDO DE
PROPIEDADES SENCILLAS PARA SER MENCIONADAS PERO VA A RESULTAR QUE UN SORPRENDENTE
NUMERO DE DIVERSOS HECHOS IMPORTANTES SE OBTENDRA COMO CONSECUENCIA DE LAS QUE
VAMOS A DESTACAR DE LAS DOCE PROPIEDADES QUE VAMOS A ESTUDIAR EN ESTE CAPITULO LAS
NUEVE PRIMERAS SE REFIEREN A LAS OPERACIONES FUNDAMENTALES DE SUMA Y MULTIPLICACION
AHORA VEAMOS LO QUE DICE PISKUNOV UNO DE LOS CONCEPTOS FUNDAMENTALES DE LAS
MATEMATICAS ES EL NUMERO EL CONCEPTO DE NUMERO SURGIO EN LA ANTIGUEDAD AMPLIANDOSE
Y GENERALIZANDOSE CON EL TIEMPO LOS NUMEROS ENTEROS T FRACCIONES SE LLAMAN NUMEROS
RACIONALES EL NUMERO RACIONAL PUEDE EXPONERSE COMO LA RAZON DE LOS NUMEROS ENTEROS
```

```
P Y Q TALES QUE P Y Q SON PRIMOS RELATIVOS ESTOS NUMEROS PUEDEN REPRESENTARSE POR
FRACCIONES PERIODICAS FINITAS O INFINITAS LOS NUMEROS QUE NO TIENEN UNA EXPASION
DECIMAL CICLICA SE LES LLAMA IRRACIONALES EL CONJUNTO QUE RESULTA DE LA UNION
DE LOS RACIONALES CON LOS IRRACIONALES SE LE LLAMA CONJUNTO DE LOS NUMEROS REALES
EN ESTA PARTE EVADE EL AUTOR TOCAR EL PUNTO DONDE SE CONSTRUYEN LOS NUMEROS REALES
LA CONCLUSION ES QUE NINGUN LIBRO DE CALCULO LO TRATARA PUES ES VERDAD SOLO NOS
IMPORTA LA COMPLETEZ DE LOS NUMEROS REALES PARA ASEGURAR QUE EXISTAN LOS LIMITES
```

6. Descifrar el siguiente mensaje que fue encriptado con Hill y se tiene la siguiente información: 'vectorial real sobre el campo de los numeros r',proviene de: LG DP XF QQ EZ II TQ RT DY RN EE PT VB RN MW BC GO XM FN. Debes proporcionar la matriz de cifrado y la matriz de decifrado.

   Con la información que se cuenta y suponiendo que el alfabeto es módulo 26, tenemos las siguiente tabla, donde las primeras dos columnas corresponden al texto claro y su vector asociado y las últimas dos columnas al texto cifrado y su vector asociado. Es decir, cada fila de la tabla indica la tranformación de texto claro a texto cifrado.

Claro	**Vector**	**Vector**	**Cifrado**
C A	(2 0)	(4 4)	E E
M E	(12 4)	(6 14)	G O
N U	(13 20)	(1 2)	B C

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 2 \\ 0 \end{pmatrix} \equiv \begin{pmatrix} 4 \\ 4 \end{pmatrix} \pmod{26}$$

Por lo que tenemos las siguientes congruencias:

$2a \equiv 4 \pmod{26} \Rightarrow a \equiv 2 \pmod{13}$

$2c \equiv 4 \pmod{26} \Rightarrow c \equiv 2 \pmod{13}$

$\therefore a = 2 + 13k_1$, $c = 2 + 13k_2$, donde $k_1, k_2 \in \{0, 1\}$ ...(A)

Por otro lado, también tenemos que: $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 12 \\ 4 \end{pmatrix} \equiv \begin{pmatrix} 6 \\ 14 \end{pmatrix} \pmod{26}$

Por lo anterior y las ecuaciones de la condición (A) se obtiene lo siguiente:

$12a + 4b \equiv 6 \pmod{26}$
$\Rightarrow 6(2 + 13k_1) + 2b \equiv 3 \pmod{13}$
$\Rightarrow 12 + 78k_1 + 2b \equiv 3 \pmod{13}$
$\Rightarrow 0k_1 + 2b \equiv -9 \pmod{13}$
$\Rightarrow (-6)2b \equiv (-6)4 \pmod{13}$
$\Rightarrow b \equiv -24 \pmod{13}$
$\Rightarrow b \equiv 2 \pmod{13}$

De manera análoga,
$\Rightarrow 12c + 4d \equiv 14 \pmod{26}$
$\Rightarrow 6(2 + 13k_2) + 2d \equiv 7 \pmod{13}$
$\Rightarrow 12 + 78k_2 + 2d \equiv 7 \pmod{13}$
$\Rightarrow (-6)2d \equiv (-6) - 5 \pmod{13}$
$\Rightarrow d \equiv 30 \pmod{13}$
$\Rightarrow d \equiv 4 \pmod{13}$

$\therefore b = 2 + 13k_3, d = 4 + 13k_4$, donde $k_3, k_4 \in \{0, 1\}...(B)$

Entonces, por las condiciones (A) y (B) sabemos que a,b,c y d tienen dos valores posibles, cada uno:

$$a = \{2, 15\}, b = \{2, 15\}, c = \{2, 15\}, d = \{4, 17\}$$

Además, la información que se tiene nos dice que dichos valores deben cumplir también que:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 13 \\ 20 \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 2 \end{pmatrix} \text{ (mód 26)}$$

Por lo que evaluando las 16 posibles combinaciones, notamos que solo hay dos matrices que la cumplen:

$$A = \begin{pmatrix} 15 & 15 \\ 2 & 17 \end{pmatrix} \text{ y } B = \begin{pmatrix} 15 & 2 \\ 2 & 4 \end{pmatrix}$$

Luego, sabemos que una matriz es invertible módulo n si y sólo si el determinante de la matriz es primo relativo con n.

$$det(A) = 225 \text{ y } det(B) = 56$$

$\therefore A$ es la única matriz que cumple todas las condiciones.

Es decir, $a = 15, b = 15, c = 2, d = 17$ corresponde a la matriz de cifrado. Para obtener la matriz de descifrado calculamos la inversa:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 15 & 15 \\ 2 & 17 \end{pmatrix}^{-1} = \frac{1}{225} \begin{pmatrix} 17 & -2 \\ -15 & 15 \end{pmatrix}^{T} = 23 \begin{pmatrix} 17 & -15 \\ -2 & 15 \end{pmatrix} = \begin{pmatrix} 1 & 19 \\ 6 & 7 \end{pmatrix} \quad \text{(mód 26)}$$

$\therefore \begin{pmatrix} 1 & 19 \\ 6 & 7 \end{pmatrix}$ (mód 26) es la matriz de descifrado.

VV RN SA GO JV DY NN HC LO XF
OM RE UT YG NE JR MO BW JF UC
KF JF DD II XY PE VV JW XK SG
IH TZ BW UK VV UK KU BW JW BB
TJ DL AQ TG TG NZ PP AY TZ GE
PJ UY KS RU MU JF AO NA MO ZW
DL DQ UK PP SC EI DL EE BW RM
BF EI SU HI JF BW RM BF EI SU
LG DP XF QQ CV RN MW BC GO XM
FN II RM UE RT DY RN EE PT VB
RN MW BC GO XM FN EI SU NA RM
SA NE OO RM YM VQ BF EI SU BW
JM GO XU SU DG KH DD PB RV VD
YW MW UP VD UI QY RM BF EI SU
LG DP XF QQ EZ II TQ RT DY RN
EE PT VB RN MW BC GO XM FN EI
SU NA RM SA YM VQ BF EI SU LG
DP XF QQ CV BH OM VV AQ PP DD
NQ DG ZM BW FI JF RM MM MD LO
GO XM JF HC YY BW SC RE UK MW
HI JF SC WW AQ TG JK NA BW AC
JV VI UK PP ZO TE JF BW ZM KL
MQ DS SG NN VK SB UG YW MW JF
HC XF GE GM WE JM MU UI WK KH
BB UK PP JF ZC VQ JF PS VV OU
WE YM CK IV RN SC BB RU ZU DY
BF EI SU LM GE SU TI UT BB JP
TZ BW AC JV VI BU WE RN SC RE
UK VB RN MW BC GO XM FN II RM
SA DJ BH OM VV AQ PP DD NQ DG
ZM MO KF QY NE YW TI BW LA XX
MK DL MW VI UK PP JF SC JW JP
II DL YW KG SA RI ZV JW GO NQ
FS PC VV JW OM MY VV BW BB LM
RI DD JF ZC VQ JF RN SG JF DL
TZ FP DD JP GK AY KS GD BB UK
PP JF LB JF OO VK VV VI BZ BW
VK AQ AO JF OC PE AE DL MW YG
WJ MK DL XF II WJ KS JV PR IQ
VQ VU VV DL TZ VB DL QG EX BH
MW AC JV VI PC UI DL QG EX HT
DY XX KS JV PR IQ VQ VU VV DL
TZ VB DL QG EX BH MW PV FP DD
QQ BN XM LM RI SU NA RM NE OO
TQ BH FP DD QQ GI AC BB GK OO
GZ MW QY DQ XY DT IQ ID QG EX
HT DY GC MU XM SG NN VK RN BC
GO XM DY JF PE SC ZM PC VV RN
UC VQ VI VK BW VI BZ BW UP SC
SC ZM JP II FG BH SC UG EU MD
VD EI TZ NN MK DL TX LO AC FB
MW LG DP XF SC UC VQ VI VK DY
DJ RN KU OM MY VV SC BW LA HR
BB UK PP JF SC MO WF DD II HS
VV HC DD BW ZU GZ YG ML SC KU
RF WS BB EI NN PS TG JM KH DD
PB TZ LB MQ BQ DY TP DD II HS
VV HC DD BW ZU GZ YG ML SC BW
RM BF EI SU LG DP XF QQ CV RN
MW BC GO XM FN II RM UE RT DY
LA XX MK DL MW VI UK PP JF SC
KU ZV TZ OM VV AQ PP BW RM BF
EI SU BW LA XX MK DL MW DY JF
SC MO KF RN MW VI UK PP JF SC
SC BW JM GO XU SU DG KH DD PB
IQ VQ SA DD JV NN HC GO MH UG
BB HC UI ZD KU VD EI PP RN SC
RE UK VB RN KU LM RI SU VQ OS
PP PS BC KU MO KF QY NE PP TU
ML VB RN MW BC GO XM FN II RM
GC GO YM HG SU JW JP II BW VV
ZH HL ZM DY VQ BF EI SU DJ BH
OM VV AQ PP DD NQ DG ZM BQ YY
GZ ZJ BB UK PP SC UI UG VV DL
VV BB YM XS BF EI SU VV BB SC
RE UK VB BH OM VV AQ PP DD NQ
DG ZM

Operando con la matriz de descifrado obtenemos el siguiente texto:

EN EL SEMESTRE ANTERIOR IMPARTI EL CURSO DE ALGEBRA LINEAL UNO EN LA FACULTAD DE CIENCIAS
DE LA UNIVERSIDAD AUTONOMA DE MEXICO E HICE ALGUNAS OBSERVACIONES ACERCA DEL
ESPACIO DUAL DEL ESPACIO VECTORIAL DE LOS NUMEROS REALES SOBRE EL CAMPO DE LOS NUMEROS
RACIONALES EL CUAL ES UN ESPACIO DE DIMENSION INFINITA PARA MOSTRAR QUE EL ESPACIO VECTORIAL REAL
SOBRE EL CAMPO DE LOS NUMEROS RACIONALES ES UN ESPACIO VECTORIAL DE DIMENSION INFINITA DEBIA
LLEGAR PRIMERO AL TEMA DE ESPACIOS DUALES Y ASI DAR UNA DEMOSTRACION FORMAL DE TAL HECHO CUANDO
LLEGAMOS AL TEOREMA QUE DICE QUE UN FUNCIONAL LINEAL TIENE QUE SU KERNEL ES UN HIPERESPACIO
FUE MI OPORTUNIDAD DE MOSTRAR QUE EL ESPACIO DE LOS NUMEROS REALES ES DE DIMENSION INFINITA
SOBRE EL CAMPO DE LOS NUMEROS RACIONALES LA IDEA ERA MUY SENCILLA ME FIJABA EN LA IMAGEN DE UN
FUNCINAL LINEAL EL CUAL ERA DEFINIDO COMO EL FUNCIONAL EVALUADO EN RAIZ DE DOS IGUAL A UNO
Y CERO SI EL NUMERO REAL NO ESTABA EN EL GENERADO DE RAIZ DE DOS MOSTRABA QUE RAIZ DE TRES
NO ESTABA EN EL GENERADO DE RAIZ DE DOS Y DEFINIA OTRO FUNCIONAL EL CUAL SE DEFINIA COMO UNO CUANDO
SE EVALUAVA EN RAIZ DE TRES Y CERO CUANDO EL NUMERO REAL NO ESTABA EN EL GENERADO DE RAIZ
DE TRES ESTA IDEA PUEDE SEGUIR PARA CADA NUMERO PRIMO Y LOS VECTORES GENERADORES

```
DE LAS IMAGENES DE LOS FUNCIONALES SON LINEALMENTE INDEPENDIENTES ASI HAY UNA  CANTIDAD INFINITA
DE VECTORES LINEALMENTE INDEPENDIENTES DEL ESPACIO VECTORIAL DE LOS NUMEROS
REALES SOBRE LOS NUMEROS  RACIONALES ASI LA DIMENSION DEL ESPACIO  DE LOS NUMEROS
REALES SOBRE LOS RACIONALES ES DE DIMENSION INFINITA EN ESE INSTANTE ME
PREGUNTE QUE PASARA CON EL ESPACIO DE LAS FUNCIONES CONTINUAS SOBRE EL CONJUNTO DE
LOS NUMEROS REALES Y ME SURGIO LA IDEA DE ENCRIPTAR EN ESPACIOS DE DIMENSION
INFINITA TOMANDO FUNCIONES QUE GENEREN UN SUBESPACIO EN UN ESPACIO DE DIMENSION INFINITA
```

El siguiente script de Python fue utilizado para descifrar el texto:

```python
import numpy as np
import sys

def descifra_hill(archivo):
    g = open('descifrado.txt','x')
    f = open(archivo,'r')
    text = f.readlines()
    x = []
    for line in text:   # Este bloque le da el formato adecuado al archivo.
        a = line.replace('\n','')
        a = a.split('&')
        if(len(a)> 1):
            x.append(a)
    count = 1
    for elem in x:
        count += 1
        for tup in elem:
            tup = tupla(tup[0],tup[1])
            a = np.matrix('1 19;6 7')  # matriz de descifrado
            b = np.matrix(str(tup[0])+';'+str(tup[1]))
            c = (a*b)%26
            a = alf[int(c[0])]+alf[int(c[1])]
            g.write(a)
            if (count % 5 == 0):
                count = 1
                g.write('\n')
```