Universidad Nacional Autónoma de México

Facultad de Ciencias

Criptografía y Seguridad

Tarea 1

Sebastián Alamina Ramírez - 318685496

Camila Alexandra Cruz Miranda - 316084707

Carlos Alberto Desiderio Castillo - 312183839

Trabajo presentado como parte del curso de **Criptografía y Seguridad**, impartido por el profesor **Manuel Díaz Díaz** durante el semestre 2023-1 en la Facultad de Ciencias, UNAM.

Fecha de entrega: **23:59 viernes 16 de septiembre del 2022**.

1. Explique brevemente por qué en $\mathbb{Z}_n$, dados $a \cong b \pmod{n}$ y $c \cong d \pmod{n}$, se tiene que $ac \cong bd \pmod{n}$.

   Solución: Supongamos $a \cong b \pmod{n}$ y $c \cong d \pmod{n}$. **PD**: $bd - ac = nk$ con $k \in \mathbb{Z}$...

   Por un lado, $a \cong b \pmod{n} \implies b - a = nk_1$ con $k_1 \in \mathbb{Z} \implies (b-a)d = nk_1 d$.
   Por otro lado, $c \cong d \pmod{n} \implies d - c = nk_2$ con $k_2 \in \mathbb{Z} \implies (d-c)a = nk_2 a$.

   Así, $(b-a)d + (d-c)a = nk_1 d + nk_2 a \implies bd - ad + ad - ac = n(k_1 d + k_2 a) \implies bd - ac = n(k_1 d + k_2 a)$.
   Haciendo $k = k_1 d + k_2 a$, llegamos a $bd - ac = nk$ con $k \in \mathbb{Z}$. ■

2. Resuelva el siguiente sistema de congruencia en caso de tener solución, en caso contrario justifique por qué no tiene solución.

$$x \cong 25 \pmod{35} \tag{1}$$
$$x \cong 15 \pmod{65} \tag{2}$$
$$x \cong 10 \pmod{15} \tag{3}$$
$$x \cong 35 \pmod{55} \tag{4}$$
$$x \cong 55 \pmod{85} \tag{5}$$

   Solución: Primero, verificamos si el sistema tiene solución, lo cual se da si y sólo si cada par de congruencias tiene solución común y, además, todas las soluciones son congruentes módulo el mínimo común múltiplo.

   - Las ecuaciones 1 y 2 tienen solución común pues $(65, 35) = 5$ divide a $15 - 25 = -10$.
   - Las ecuaciones 1 y 3 tienen solución común pues $(15, 35) = 5$ divide a $10 - 25 = -15$.
   - Las ecuaciones 1 y 4 tienen solución común pues $(55, 35) = 5$ divide a $35 - 25 = 10$.
   - Las ecuaciones 1 y 5 tienen solución común pues $(85, 35) = 5$ divide a $55 - 25 = 30$.
   - Las ecuaciones 2 y 3 tienen solución común pues $(15, 65) = 5$ divide a $10 - 15 = -5$.
   - Las ecuaciones 2 y 4 tienen solución común pues $(55, 65) = 5$ divide a $35 - 15 = 20$.
   - Las ecuaciones 2 y 5 tienen solución común pues $(85, 65) = 5$ divide a $55 - 15 = 40$.
   - Las ecuaciones 3 y 4 tienen solución común pues $(55, 15) = 5$ divide a $35 - 10 = 25$.
   - Las ecuaciones 3 y 5 tienen solución común pues $(85, 15) = 5$ divide a $55 - 10 = 45$.
   - Las ecuaciones 4 y 5 tienen solución común pues $(85, 55) = 5$ divide a $55 - 35 = 20$.

   Luego, procedemos a resolver; sean $k_i \in \mathbb{Z}$ para $1 \leq i \leq 5$...

   Empezamos obteniendo x de la congruencia con el módulo más grande (i.e. la $5^{\underline{a}}$).
   $$x \cong 55 \pmod{85} \implies x = 55 + 85k_1.$$
   Sustituyendo (y simplificando) en la siguiente congruencia de módulo más grande (i.e. la $2^{\underline{a}}$)...
   $$x \cong 15 \pmod{65}$$
   $$55 + 85k_1 \cong 15 \pmod{65}$$
   $$85k_1 \cong (15 - 55) \pmod{65}$$
   $$20k_1 \cong 25 \pmod{65}$$
   Mediante un pequeño análisis (o mediante el Algorimo de Euclides), observamos que $gcd(20, 65) = 5$.
   Luego, como $25\%5 = 0$, esta congruencia tiene solución. Procedemos a dividir todas sus partes entre este máximo común divisor, y multiplicar de forma tal que la congruencia pueda ser simplificada...
   $$4k_1 \cong 5 \pmod{13}$$
   $$(10)4k_1 \cong (10)5 \pmod{13}$$
   $$40k_1 \cong 50 \pmod{13}$$
   $$k_1 \cong 11 \pmod{13}$$

De aquí obtenemos k_1, que sustituimos en la x obtenida previamente.

$$k_1 = 11 + 13k_2$$
$$x = 55 + 85k_1$$
$$x = 55 + 85(11 + 13k_2)$$
$$x = 55 + 935 + 1105k_2$$
$$x = 990 + 1105k_2$$

Procedemos sustituyendo esta nueva x en la siguiente congruencia de módulo más grande (i.e. la $4^{\underline{a}}$).

$$x \cong 35 \pmod{55}$$
$$990 + 1105k_2 \cong 35 \pmod{55}$$
$$1105k_2 \cong (35 - 990) \pmod{55}$$
$$5k_2 \cong 35 \pmod{55}$$
$$\big(gcd(5, 55) = 5 \ \wedge \ 35\%5 = 0\big) \implies k_2 \cong 7 \pmod{11}$$
$$\implies k_2 = 7 + 11k_3$$
$$\implies x = 990 + 1105(7 + 11k_3)$$
$$\therefore x = 8725 + 12155k_3$$

Procedemos con la $1^{\underline{a}}$ congruencia.

$$x \cong 25 \pmod{35}$$
$$8725 + 12155k_3 \cong 25 \pmod{35}$$
$$12155k_3 \cong (25 - 8725) \pmod{35}$$
$$10k_3 \cong 15 \pmod{35}$$
$$\big(gcd(10, 35) = 5 \ \wedge \ 15\%5 = 0\big) \implies 2k_3 \cong 3 \pmod{7}$$
$$2k_3 \cong 3 \pmod{7}$$
$$4(2)k_3 \cong 4(3) \pmod{7}$$
$$k_3 \cong 5 \pmod{7}$$
$$\implies k_3 = 5 + 7k_4$$
$$\implies x = 8725 + 12155(5 + 7k_4)$$
$$\therefore x = 69500 + 85085k_4$$

Finalmente, trabajamos con la congruencia restante (i.e. la 3).

$$x \cong 10 \pmod{15}$$
$$69500 + 85085k_4 \cong 10 \pmod{15}$$
$$85085k_4 \cong (10 - 69500) \pmod{15}$$
$$5k_4 \cong 5 \pmod{15}$$
$$\big(gcd(5, 15) = 5 \ \wedge \ 5\%5 = 0\big) \implies k_4 \cong 1 \pmod{3}$$
$$\implies k_4 = 1 + 3k_5$$
$$\implies x = 69500 + 85085(1 + 3k_5)$$
$$\therefore x = 154585 + 255255k_5$$

Por lo que esta última x es la solución al sistema.

En notación de congruencia lineal, tenemos:

$$x \cong 154585 \pmod{255255}$$

■

3. El siguiente texto fue cifrado en mono alfabético, realice un análisis de frecuencias tomando en cuenta que los caracteres están en correspondencia de la siguiente forma a=0, ..., z=25, no hay acentos ni ñ.

   Encuentre la clave y descifre el mensaje.

IL NPMTRFKL QNFHR ERI QLPQSMVEMQ QR RQTL LELNTLKEM ERAFEM L NPRQFMKRQ QRIRSTFVLQ IL RQSLIL CIMALI ER IL NLKERJFL ER SMVFE DL ERJMQTPLEM IL RVMIUSFMK ERI QLPQSMVEMQ Y ILQ SILVRQ ER LELNTLSFMK. ERQNURQ ER SLTMPSR JRQRQ ERQER IL ERSILPLSFMK ER IL NLKERJFQ, JUITFNIRQ VLPFLKTRQ DLK QUPCFEM Y QR DLK BFGLEM RK IL NMAILSFMK DUJLKL CPLSFLQ L RXTPFKQRSLQ NPRQFMKRQ QRIRSTFVLQ QF KM TLJAFRK L IL SLNLSFELE JUTLSFMKLI FKDRPKRTR ERI VFPUQ. LOUF LNIFSLJMQ UKL NPURAL ER RVMIUSFMK ER QUQTFTUSFMK KRUTPL L IL NPMTRFKL ER NFSM ER IL NPMTRFKL MJFSPMK Y QR SMJNLPM L IL RVMIUSFMK KRUTPL ER IL VLPFRKTR ER NPRMSUNLSFMK ER IMQ ERJLQ. PRLIFZLJMQ SMJNLPLSFMKRQ RKTPR ILQ FKTRPLSSFMKRQ RKTPR ILQ NPMTRFKLQ Q ER IMQ SMV(LIBL,RTL,CLJJL,ERITL Y MJFSPMK) Y RI PRSRNTMP LSREMQ. IMQ LJFKMLSFEMQ SMJNLPTFEM RKTPR TMELQ ILQ NPMTRFKLQ Q OUR QR UKRK L LSREMQ NRPJLKRSRK SMKQTLKTRQ IM OUR FKEFSL OUR RQTMQ LJFKMLSFEMQ QMK RQRKSFLIRQ NLPL IL UKFMK NPRSFQL LI PRSRNTMP. IMQ SMJNIRGMQ PAE NLPL SLEL VLPFLTR SMK RI PRSRNTMP QR UTFIFZLPMK NLP FERKTFBFSLP IMQ LJFKMLSFEMQ FKVMIUSPLEMQ RK IL FKTRPLSSFMK NPMTRFKL NPMTRFKL. IL PAE ER MJFSPMK RQTLAIRSR MSDRKTL Y EMQ SMKTLSTMQ BPRKTR L IMQ QRQRKTLYSULTPM ER IL NPMTRFKL MPFCFKLI ER WUDLK NMP IM TLKTM, RI KUJRPM JREFM ER SMKTLSTMQ NMP PRQFEUMQ RQ JLYMP NMP IM OUR RI SMKTLSTM TRPJMEFKLJFSM RQ JLQ RQTLAIR. IMQ PAE ER IMQ SMV QMK QFJFILPRQ RK QRSURKSFL Y RQTPUSTUPL QFK RJALPCM, RI PAE ER MJFSPMK NPRQRKTL IL ERQVFLSFMK JLQ CPLKER ER IL RQTPUSTUPL NMP UKM NUKTM MKSR LPJQE, SLUQLEM NMP UK SMKGUKTM ER JUTLSFMKRQ SRPSLKLQ L IL CIFSMQFILSFMK KTPRQFTKRM SULPRKTL Y TPRQ ER IL NPMTRFKL MJFSPMK Q QMK EFBRPRKTR ER IL NPMTRFKL MPFCFKLI OUR NPMVMSLK UK PRSMKMSFJFRKTM PREUSFEM NMP NLPTR ER IMQ LKTFSURPNMQ KRUTPLIFZLKTRQ. KURQTPMQ PRQUITLEMQ QUCUFRPRK OUR ILQ NPRQFMKRQ QRIRSTFVLQ QMK FKEUSFELQ NMP IL VLSUKLSFMK JLQFVL RK TMEM RI JUKEM Y NMP NRPQFQTRKSFL ER FKBRSSFMRQ PRSUPPRKTRQ RK FKEFVFEUMQ FKJUKMERNPFJFEMQ, OUR KM RIFJFKLPMK IL FKBRSSFMK Y LSLALPMK BLSFIFTLKEM IL QRIRSSFMK ER VFPUQ SUYLQ SLPLSTRPFQTFSLQ QMK EFBRPRKTRQ L IMQ SMV LKTRPFMPRQ, JRKMQ NLTMCRKMQ NRPM SMK JLYMP TPLKJFQFAFIFELE.

Solución: Primero, realizamos la tabla de frecuencias de los símbolos en el texto cifrado.

Letra	Frecuencia	Porcentaje
A	14	0.8%
B	9	0.5142857142857142%
C	11	0.6285714285714286%
D	7	0.4%
E	90	5.142857142857142%
F	132	7.542857142857143%
G	3	0.17142857142857143%
H	1	0.05714285714285715%
I	88	5.028571428571428%
J	46	2.6285714285714286%
K	141	8.057142857142857%
L	200	11.428571428571429%
M	172	9.828571428571427%

Letra	Frecuencia	Porcentaje
N	56	3.2%
O	8	0.4571428571428572%
P	117	6.685714285714285%
Q	142	8.114285714285714%
R	210	12.0%
S	108	6.171428571428572%
T	92	5.257142857142857%
U	60	3.428571428571429%
V	24	1.3714285714285714%
W	1	0.05714285714285715%
X	1	0.05714285714285715%
Y	14	0.8%
Z	3	0.17142857142857143%

Sospechamos que este texto está en español (mod 26) y que se ha conservado la separación de las palabras del texto original (también en español).

Notemos que en el texto cifrado hay varias palabras de **una** sola letra: `L, Y, Q`, las cuales podrían ser las vocales "a, e, o, u" y la letra "y" debido a que son las palabras de una sola letra que encontramos en el español, pero notamos que la letra **L** en el texto cifrado es la segunda letra más frecuente en el texto, así como en general, la letra **a** es la segunda más frecuente en el español, además que es más probable que sirva como conectivo de dos palabras, por lo que tomemos que la letra **L** esta cifrada con la letra **a**, y que la letra más frecuente del texto cifrado que es la **R**, pensemos que es la letra **e**.
teniendo así las primeras 2 letras:

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
L	-	-	-	R	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

Luego encontramos palabras de **dos** letras: `IL, QR, ER, DL, RK, QF, RI, IM, LI, RQ, UK, KM`, si tomamos que la letra **e** se cifró con la letra **R**, entonces las palabras `QR, ER` serian las palabras `se, de` en el texto original, que son las palabras más usuales de dos letras que terminan en **e**, así **Q** es **s** ó `d`, lo mismo para **E**, pero teniendo la palabra cifrada **ERQNURQ**, sustituyendo la letra **R** por la **e** y la letra **Q** por **s** tenemos la palabra **EesNUes**, en este tipo de cifrados, las ultimas letras del abecedario no tienen cambios, por lo que es probable que la letra **U** se cifre así misma, y que la letra **E** debe ser la que cifre la letra **d**, y la **N** a la **p**, para tener la palabra **después**.

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
L	-	-	E	R	-	-	-	-	-	-	-	-	-	-	N	-	-	-	-	U	-	-	-	-	-

Ahora con la palabra cifrada **JRQRQ**, al sustituir las letras que ya encontramos tenemos la palabra **Jeses**, que es muy seguro que la palabra original sea **meses**, así la letra **J** cifra a la letra **m**, por lo que nuestras letras descubiertas al momento son:

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
L	-	-	E	R	-	-	-	-	-	-	-	J	-	-	N	-	-	Q	-	U	-	-	-	-	-

Ahora analizando la palabra cifrada **RQSLIL**, al sustituir las letras que conocemos, tenemos la palabra **esSaIa**, que parece ser que la palabra original es **escala**, por lo que la letra **S** cifra a la letra **c**, mientras que la **I** a la letra **l**, con esto, nuestras letras descubiertas son:

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
L	-	S	E	R	-	-	-	-	-	-	I	J	-	-	N	-	-	Q	-	U	-	-	-	-	-

Donde se puede ver que la palabra clave parece ser **LASER**, sí acomodamos el abcedario con la palabra clave al inicio, tenemos ya descubiertas todas las letras, y el abcedario que se uso para encriptar el mensaje, que es el siguiente:

Abecedario descifrado:

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

Texto descifrado:

LA PROTEINA SPIKE DEL SARSCOVDOS SE ESTA ADAPTANDO DEBIDO A PRESIONES SELECTIVAS LA ESCALA GLOBAL DE LA PANDEMIA DE COVID HA DEMOSTRADO LA EVOLUCION DEL SARSCOVDOS Y LAS CLAVES DE ADAPTACION. DESPUES DE CATORCE MESES DESDE LA DECLARACION DE LA PANDEMIS, MULTIPLES VARIANTES HAN SURGIDO Y SE HAN FIJADO EN LA POBLACION HUMANA GRACIAS A EXTRINSECAS PRESIONES SELECTIVAS SI NO TAMBIEN A LA CAPACIDAD MUTACIONAL INHERNETE DEL VIRUS. AQUI APLICAMOS UNA PRUEBA DE EVOLUCION DE SUSTITUCION NEUTRA A LA PROTEINA DE PICO DE LA PROTEINA OMICRON Y SE COMPARO A LA EVOLUCION NEUTRA DE LA VARIENTE DE PREOCUPACION DE LOS DEMAS. REALIZAMOS COMPARACIONES ENTRE LAS INTERACCIONES ENTRE LAS PROTEINAS DE LOS COV(ALFA,ETA,GAMMA,DELTA Y OMICRON) Y EL RECEPTOR ACEDOS. LOS AMINOACIDOS COMPARTIDO ENTRE TODAS LAS PROTEINAS S QUE SE UNEN A ACEDOS PERMANECEN CONSTANTES LO QUE INDICA QUE ESTOS AMINOACIDOS SON ESENCIALES PARA LA UNION PRECISA AL RECEPTOR. LOS COMPLEJOS RBD PARA CADA VARIATE CON EL RECEPTOR SE UTILIZARON PARa IDENTIFICAR LOS AMINOACIDOS INVOLUCRADOS EN LA INTERACCION PROTEINA PROTEINA. LA RBD DE OMICRON ESTABLECE OCHENTA Y DOS CONTACTOS FRENTE A LOS SESENTAYCUATRO DE LA PROTEINA ORIGINAL DE WUHAN POR LO TANTO, EL NUMERO MEDIO DE CONTACTOS POR RESIDUOS ES MAYOR POR LO QUE EL CONTACTO TERMODINAMICO ES MAS ESTABLE. LOS RBD DE LOS COV SON SIMILARES EN SECUENCIA Y ESTRUCTURA SIN EMBARGO, EL RBD DE OMICRON PRESENTA LA DESVIACION MAS GRANDE DE LA ESTRUCTURA POR UNO PUNTO ONCE ARMSD, CAUSADO POR UN CONJUNTO DE MUTACIONES CERCANAS A LA GLICOSILACION ENTRE SIETE O CUARENTA Y TRES DE LA PROTEINA OMICRON SON DIFERENTE DE LA PROTEINA ORIGINAL QUE PROVOCAN UN RECONOCIMIENTO REDUCIDO POR PARTE DE LOS ANTICUERPOS NEUTRALIZANTES. NUESTROS RESULTADOS SUGUIEREN QUE LAS PRESIONES SELECTIVAS SON INDUCIDAS POR LA VACUNACION MASIVA EN TODO EL MUNDO Y POR PERSISTENCIA DE INFECCIOES RECURRENTES EN INDIVIDUOS INMUNODEPRIMIDOS, QUE NO ELIMINARON LA INFECCION Y ACABARON FACILITANDO LA SELECCION DE VIRUS CUYAS CARACTERISTICAS SON DIFERENTES A LOS COV ANTERIORES, MENOS PATOGENOS PERO CON MAYOR TRANMISIBILIDAD.

4. El siguiente cifrado es implementado en Vigenère, los caracteres fueron puestos en una biyección del 0 al 25 donde a=0 y 25=z. Sin signos de puntuación ni ñ.

   Aplique la prueba de Kasiski de la longitud de la clave, la clave, y después descifre el mensaje.

   El mensaje está dividido en bloques de tres.

PNX ARW UZI EWA LMA ZRT MYZ DBI EPA EQM LEE UVW AZZ BLG TZE LLH ACZ CHA CPL HAE ZJH AQP MBB VLQ NML LEL BNX EWQ BNA EDN OEL XHP SEW FWA OIY ZSL MPL LHA RDT BZN WEL PNN EVZ RAE EWF PXM QRY DXG YZS LWO LHT AGL TKI ADF HZZ LRE IRD CTA NNA UMY WEK IQP MBB VLE GCA PDB NVN IHL RQA GBN DIT LRG AKQ BDP BAB DCH VEF LHA ETS HAP LIK MYP SRZ BDE MWA PSE WUZ RGM NOU KIA EET TTF NTA UZR TAR YEE ARN AWW EJD XAC FEL TBC OVQ NNO GAV PTX TVE RHA QPL TKN AAK IQL REM STR FMM LYL WFE EGI FFC KMN NIH VRW DBI QPL TJB OAF QGT AET RRO TVH PSM ZNN ALI PZN NVC PIG IQZ QNM ZPD BIQ ZSF MGC OLL RLL MCE LSX DRT ABU CCE LQB YAG BRN UTV QZA UZV XOL TNA UXZ GLP TZN DAE QED EXA PFC AWH YZN UOT DHI YWE OIA EAK TNG ILB NLL VQR WOW MFN UUZ VXO LCA MIV PBB UXA RLC XZP LBT DBW AGL BLT HLN GEE WPT DTL DFE XAR DOI ZRR UGB BXI FIZ LYH ARW OJC RPS TKY LRX BET UGN NWC NIA OOE WCF DXL VDT BVT FIK UND DXK RCC TMF FNF ILL TXG RDO JCR PSB VGP RKW TZM BPR CMT VNF NFI LLT XTR DIG NBC MXM FFN TMF AEV QRO EXA PLR TJN UOI MEZ UGX BNO FIF CEV PBY CAW RWM TGN EEX ZNO EEU VDM HKB WOK ZBU OUZ VWL TVG PQN MRW CTJ RWL HLR XIM QNP LBV FPC MWI ZLH MAA IVI QLY SIB DES IZM UET BPN XTC PIG IQZ ARY HPA LKB RRB BBX IFI ZLA RYH PSN AGZ BXZ EPO FQU PRF IAL ARY HPB TZO LRB LNO SXP VDT XZV KOF QGT AJC VEE GUR WOI MEZ SBV QPS VWZ AOG MEP LIM VYA WWN OVB ZGT OGW FLS HUN XOL BRX EKW FZS TTN DPK WSF NWQ QLD XAQ PEL IFP LOI EZJ TGN WOO QQT JHU VAA IIR DTT CAA OVW NEU KLV OOR UNC ETL BAO KMY ZLH ZQP LTT NNA LIY OET PVP LFI LLT XVB ZBX LRN IHT RXE MQZ ZSN VYL PBH UFR ZIZ ZSV WAP LWM QZL XAB ALT UBD YGI QLE EXR TNT LBD EZC VLI GBN NTH IQP NMZ BOE GIQ LVT TVP RHV FFP EQP LST URY ASI FYI EWF XAL ZHO OLX EZC XLV XIX VGZ SGQ ZZD HAR TMI IPT EGB BXI IIC LSX VBD HTK REA KLR EEG LEL SJC RTR VWA PSH UVE ITI HYQ NMA PRO QBD ALI OTA JCR YOM MAT AHB ELA EBR CNT BVG AEI STE LBN ERT VFN UKZ VLN HZZ LLF MAE EIM EZM BBV LSX ABM RXA NWT TJN LCT LNC AMW PFA GLB EEK UVY AFW FOE VMA LRR MZA ESW YLM NAV NAF QGT ATP BRO NVT CIM WDF EMM CLS TTR ARX OHY TXK EPO JCR PLX APL RTJ NUO XAG LBT QYL NWW FFS NZE ZMX IFZ MXI YAE BVN OOR MSP CMQ ILM XVG PEE MFN AKI OLJ HZB UOX AGL BTJ NTL TVQ ZEE XET MXZ ILL LLR WAG WPS EHJ FPR OMS LSV QAL DHY HPE EUR CEG OHP DXT CLS MMY OEU WQL SMM ATA ZZN YDX AFP MXR NYZ TAP ZNX TCP IGI QZD XUV EIT TYP GHM YXO FMA EOW MSP LBK VEA KIY ZSG WIT OLU VEI TAR WEO IAE OVW ZZT HLB DYT TNM RTH NCA EIA ZVB IMK EEM FNA KIO LJH LRN IWQ BGO EIE PNX TVY EKQ BCD XTC PIG IQZ QNM RDE LME FIW WCC EZC AEO EIA ZVB INW GHI FFS MIQ LPT ZRN EJC RGI XVR OEM CPL BXH NEI TMF XIT XNC AMW CLR TTN DOK LRC AKM FAO GLV ZEE TNN OGC ALS HVE TST LRA AGQ PZ

Solución: Al analizar el texto cifrado, encontramos las siguientes sub cadenas o secuencias que más se repiten en el texto: HA, AE, EL y UZ, después en la siguiente tabla ordenamos la las cadenas con las distancias entre secuencias repetidas, y su mínimo común divisor entre ellas:

Secuencia	Distancias	Minimo común divisor
HA	5, 5, 5, 40, 120, 5, 85, 125	5
AE	32, 44, 103, 148, 100, 28	2
EL	211, 626, 38, 60	2
UZ	32, 225, 12, 848, 50	2

Notamos que el mínimo común divisor más frecuente es 2, seguido de 5, si la palabra clave tiene longitud de 2, seria menos segura que si lo es de longitud 5, por lo que suponemos que la longitud de la clave es de 5, y dividimos el texto cifrado en 5 cadenas, para analizar las frecuencias de letras en cada partición del texto, que esta cifrado con una misma letra.

Columna 1: La primer columna a analizar es la siguiente:

PWWZZPLWLLZPZPLLXNOPWZLDWNAPYZLLDLDNWPLPNQDGDDFTLPDPZOEFZYNJFCNPEPALTLE
FNWPOTRPNZPZPZCLLTCYNZXALDDFYTWEGLWNXMBLLWLGTFDRXLWPLTWOFDFDCFLDPPZCFL
DCFAOLUZNCYWEODWUWPWWXPPZALDMPPZPRXLPZPPLPLODKTEWZPAPYOTLXXZDFLPPZWTAD
AEOCAZPNOPLZNXZLFZPZADLTDLNPOLPFLYYXOZXZZTTXLDEELTPEYPDTYTLCGTENLLEZLMWLC
FEYOLALNTR.

Realizamos su respectivo análisis de frecuencias, para encontrar la posible letra con la que se cifró el texto, y asumiendo que es un texto en español, se encontró que las letras más frecuentes en esta columna son **L** y **P**, que son candidatas a que se haya usado la letra **e** para su cifrado, en ambos casos buscamos en la tabla de Vigenère, en la columna **E**, donde se intersectan en las letras **L** y **P**, y encontramos que las letras candidatas para la prumera letra de la clave son **H** y **L** respectivaente.

La siguente tabla es el resultado del análisis de frecuencias de cada letra en la columna uno, de un lado se muestra cada una de las letras y a un lado se muestra su respectiva frecuencia con la que apareció en la columna uno:

Letra	Frecuencia en porcentaje
A	4.4%
B	0.40%
C	4%
D	9.23%
E	1.2%
F	6.02%
G	1.60%
H	0%
I	0%
J	.40%
K	.40%
L	18.47%
M	1.20%

Letra	Frecuencia en porcentaje
N	6.42%
O	5.22%
P	16.06%
Q	.4%
R	1.60%
S	0%
T	7.22%
U	.8%
V	0%
W	8.03%
X	4.81%
Y	4.4%
Z	11.64%

Columna 2: La segunda columna a analizar es la siguiente:

NUARDAEAGLCLJMQEEAESASLTEEEXDSHTFRCAEMEDIAIAPCLSISESRUENREADEOOTRLARRYECI
DLAAOSANIQDSOLSAEAUAOUPAECZDEAILOUOIUCBATEDEOUIYOSRUCODTIDCNTOSRMMNTIMNEE
ROUOECMEEMOOLQCLILCLIYEUNIAARIASBORABRSTOAEOSSOLAVOSOESPNDELJOJATOUOEOLLA
ELTBIESPRSLLLYENEITNEVRPSAIAOCISDMEISHAESRSIQRAAOAANAERUNLEMSRTCAAEAEREMAAO

Al realizar el análisis de frecuencias notamos que las 2 letras más frecuentes son **A** y **E**, de donde si buscamos en la tabla de Vigenère, en la columna **E**, las posibles letras de la clave que se usaron, tenemos como candidatas **W** y **A**, pero la letra **W** es muy poco probable que aparezca en alguna palabra, por lo que las primeras letras de la clave pueden ser: **HA** ó **LA**, se muestran las frecuencias en la siguiente tabla:

Letra	Frecuencia en porcentaje
A	13.6%
B	1.36%
C	4.42%
D	4.08%
E	13.94%
F	.34%
G	.34%
H	.68%
I	6.80%
J	1.02%
K	0%
L	7.14%
M	3.40%

Letra	Frecuencia en porcentaje
N	4.08%
O	9.52%
P	1.70%
Q	1.36%
R	6.80%
S	8.50%
T	4.08%
U	4.08%
V	.68%
W	0%
X	.34%
Y	1.36%
Z	.34%

Columna 3: La tercera columna a analizar es la siguiente:

XZLTBEEZTHHHHBNLWELEOLHBLVEMXLTKHETUKBGBHGTKBHHHKRMEGKTTTEWXLVGXHTKEFLGKH
BTFETMLNGNBFLMXBLGTULXTEXANHOKLVWULVXXTGHETXIGFHJTXGNEXBKXTFXJBKBTFXGXTVX
TIGFVATXEHKUTNTHMBMHVSSEXGRLBFRNXFFRTBXXFJGIBVGIWBGHLKTKWXLOTOHITVKRTKHTLT
FXXHMNBZVWXTGETZGHMGTHETSELLXXGHIGIXTKGJVHTNOLJMHETELTKHFIBXXTTMGKFVRSNFTN

En el análisis de frecuencias vemos que las letras más frecuentes son **T** y **X**, buscando en la tabla en la columna **E**, vemos que las posibles letras que cifraron la columna son **P** ó **T**, por lo que las primeras 3 letras de la clave pueden ser: **HAP**, **HAT**, **LAP** ó **LAT**. La siguiente tabla muestra las frecuencias:

Letra	Frecuencia en porcentaje
A	.68%
B	6.46%
C	0%
D	0%
E	6.80%
F	5.10%
G	7.82%
H	9.52%
I	2.72%
J	1.70%
K	6.12%
L	7.48%
M	3.40%

Letra	Frecuencia en porcentaje
N	3.74%
O	1.70%
P	0%
Q	0%
R	2.04%
S	1.36%
T	13.94%
U	1.36%
V	4.08%
W	2.04%
X	10.54%
Y	0%
Z	1.36%

Columna 4: La cuarta columna a analizar es la siguiente:

AIMMIQUZZAAAABMBQDXWIMAZPZWQGWAIZIAMIBCNLBLQAVAAMZWWMITAAAWATQATAKIMMWI
MVIJQTVZIVIMIMLCDUQBVZTZZQAWUIITBQMZCPAZDLLWLAZBIACKBNIWLVUKMIGCVWPVITNMMQ
AJMXIPWGZUKZZVMJLQVWMIIITTIYKBIYAZQIYZLPZQCUMVWMMWZWUBWTWQAIIGQUICWLULMZ
TIPIVLTQVHIWMAUIXLCBIZITVQUIWZXLVQAIBIVKLLCWUIMQICMBBBIBVZZMMBAAJLWLUWMMWAQ

El análisis de frecuencias arroja que las letras mas frecuentes son **I** y **M**, de las cuales se deduce que las posibles letras con las que se cifro la columna son **E** y **I**, por lo que las palabras clave candidatas son: **HAPE**,**HAPI**, **LAPE** ó **LATI**, la siguiente tabla muestra las frecuencias de la cuarta columna:

Letra	Frecuencia en porcentaje
A	9.86%
B	5.78%
C	3.40%
D	1.02%
E	0%
F	0%
G	1.36%
H	.34%
I	13.92%
J	1.36%
K	2.04%
L	6.12%
M	10.40%

Letra	Frecuencia en porcentaje
N	1.02%
O	0%
P	2.38%
Q	6.80%
R	0%
S	0%
T	4.42%
U	4.42%
V	6.12%
W	8.50%
X	1.34%
Y	1.020%
Z	8.50%

Columna 5: La quinta columna a analizar es la siguiente:

REAYEMVBECCEQVLNBNHFYPRNNRFRYOGAZRNYQVAVRNRBBEEPYBAUNATURRECBNVVQNQSMFF
NRQBGRHNPCQZQGRERCBRQVNGNEPHOYANNRFVABRPBBNPDRRBZRRYENACVTNRFLRRGTRNLRB
FFRPNEBFBRNNVBBVGRRRNFIAQBZBCQHBBZHGEUAHONVVGVREQZEVNGFNRFNSQQFENQVRANV
NBYQNYVLBRRZYUZAQBBQRBVNQBQVFPRFFHEVGZRPBCBRRERAVHABORAERVSNFVZAEVBNNNP
BVFAZYVGBT

En este último análisis vemos que las letras más frecuentes son **N** y **R**, los que implica que las posibles letras con las que cifro esta columna son **J** y **N**, pero la letra **J**, no tendría sentido con las anteriores letras, por lo que tomamos la letra **N**, así las posibles palabras son: **HAPEN**, **HAPIN**, **LAPEN** y **LATIN**, la siguiente tabla muestra las frecuencias por letra:

Letra	Frecuencia en porcentaje
A	5.78%
B	11.22%
C	2.72%
D	.34%
E	6.46%
F	6.12%
G	3.74%
H	2.72%
I	.34%
J	0%
K	0%
L	1.36%
M	.68%

Letra	Frecuencia en porcentaje
N	12.24%
O	1.36%
P	3.40%
Q	6.46%
R	14.62%
S	1.02%
T	1.36%
U	1.36%
V	9.12%
W	0%
X	0%
Y	3.74%
Z	3.74%

Las únicas palabras con sentido sólo son **HAPEN** y **LATIN**, Pero tomamos como referencia desde el inicio que el texto esta en español, por lo que tomamos como palabra clave **LATIN**, y deciframos el mensaje, donde el mensaje original vendría siendo el siguiente:

EN ESE LUGAR LA SENORA ELODIA REALIZA EL MILAGRO AGARRA LOS POCOS PELOS ROJOS DE MI TIA QUE YA ESTA MEDIO CALVA DESPUES LOS LAVA LOS SECA LOS ESTIRA LES HACE CREPE LOS EXTIENDE YLOS SOBA HASTA TRANSFORMAR LA ESCASA CABELLERA DE MI TIA EN UN EDIFICIO DE FANTASIA DE VARIOS PISOS CON RULOS RISOS CAIRELES Y ROSETONES LO HORNEA DURANTE ALGUNAS HORAS EN EL SECADOR Y DESPUES LO ROCIA CON SIETE LITROS DE LACA PARA DARLE FIRMEZA Y SOSTEN A SU CREACION EL DIA DE LA BODA MI TIA LLEGO A NUESTRA CASA CON UN PEINADO QUE MEDIA DOS METROS DE ALTURA SE VEIA IMPRESIONANTE CUANDO ABRIMOS LA PUERTA PARA SALIR SE ESCUCHO UN ZUMBIDO AL LEVANTAR LA VISTA AL CIELO DESCUBRIMOS UN BICHO QUE SE ACERCABA VOLANDO A TODA VELOCIDAD QUE ES ESO PREGUNTO MI MAMA YO SE LO QUE ES ACLARE TRIUNFAL CUANDO LO PUDE DISTINGUIR MAS DE CERCA ES UN MAYATE Y ESO QUE ES INTERROGO MI HERMANA UN MAYATE LES INFORME ES UNA ESPECIE DE ESCARABAJO PERO UN POCO MAS RECHONCHO EL MAYATE ERA DEL MISMO COLOR ROJO BRILLANTE QUE EL CABELLO DE MI TIA EL INSECTO VOLO ENPICADA Y ZAO SE ZAMBULLO EN EL PEINADO AY QUE ASCO GRITO MI MAMA AY QUE SUSTO BERREO MI HERMANA AY QUE BARBARIDAD SE HISTERIZO MI TIA QUITENMELO PERO SIN DESCOMPONER EL PEINADO ADVIRTIO NOS ASOMAMOS TEMEROSOS A LAS PROFUNDIDADES DE ESA SELVA ROJA YA LO VI DIJO MI PAPA ESTA UN POCO ATURDIDO Y MAREADO POR EL OLOR DE LA LACA SAL DE AHÍ EL MAYATE NO OBEDECIO LE METIMOS UN LAPIZ HURGAMOS CON EL DEDO LE SOPLAMOS Y NADA EL PEINADO SEGUIA INTACTO ADENTRO DE NADA VALIERON SUPLICAS AMENAZAS NI LOS MAS RUDOS PROCEDIMIENTOS NI MODO SE IMPACIENTO MI PAPA SE NOS HACE TARDE TENDRAS QUE IR CON ESO MI TIA AUNQUE NERVIOSA SABIA QUE NO TENIA OTRA ALTERNATIVA LA FIESTA TRANSCURRIA NORMALMENTE PERO MI TIA SE SOBRESALTABA A CADA RATO CUANDO TERMINAMOS DE CENAR Y EMPEZO LA MUSICA MI TIA AHOGO UN GRITO QUE TE PASA LE PREGUNTE CREO QUE EL ESCARABAJO ESTA BAILANDO SUSURRO ME ASOME AL PEINADO Y EFECTIVAMENTE EL ESCARABAJO ROJO ESTABA BAILANDO EL PRIMER VALS DE LA NOCHE OBSERVE FASCINADO QUE EL MERENGUE DEL PASTEL DE BODAS TENIA GRANDES SEMEJANZAS CON EL PEINADO DE MI TIA LLEGO EL MOMENTO DE FELICITAR A LOS NOVIOS MI TIA SE LEVANTO COMO TODOS Y AL ABRAZAR A LA NOVIA ZZ EL ES CARABAJO DECIDIO VOLAR EN EL INERIOR DEL PEINADO QUE ES ESE RUIDO PREGUNTO LA NOVIA ALGO ASUSTADA PARECE QUE VIENE DE TU CABEZA TIA ES MI APARATO PARA LA SORDERA RESPONDIO ELLA CON UNA SONRISA DE PANICO.

5. El siguiente mensaje fue cifrado con el algoritmo de Hill poniendo en correspondencia a=0, ..., z=25, sin ñ ni puntos ortográficos.

   (a) Encuentre la matriz de cifrado y proporcione sólo las ecuaciones que lo llevan al resultado.

   (b) Encuentre la matriz de descifrado.

   (c) Descifre el mensaje.

   Partiendo de que se tiene la siguiente correspondencia:
   PP EK TC DW DS YA WE MI NA RS FG proviene de "El sábado fuimos a una boda".

   PP EK TC DW DS YA WE MI NA RS FG CK JD IM MA GQ XM EH QC RS FG ND DH GC EW HK WG BE BI TI LV ME OF NN RO LI OF VT FZ UG LT WQ UM YI QH MA BW WW WG SW RH EU WW TO FP UO TP QL SY QC JC PP OK JC FR LI IE WU NN PY ND DH FX EU RH IC EO OK OC DR DU MK EO XV RH QC DU ND BP WG UG DC ZH IG NA DW GI AQ QO UJ FX EU DB LD NL JT VG MK LI KU GG XY TP EO JD EQ JR DB DH RH EW HK WG BE BI DO EQ DB WG XV SM FM RY RH TP XS LO SD NF SM ZM PE

   Solución: Tomando en cuenta que se está trabajando con diagramas (i.e. $N = 2$) tenemos que la matriz K de cifrado es de la forma $K = \begin{pmatrix} k_{1,1} & k_{1,2} \\ k_{2,1} & k_{2,2} \end{pmatrix}$.
   Sabemos que el par **BA** se cifra a **TC**, es decir el vector $(1, 0)$ al aplicarle la matriz K va al vector $(19, 2)$, si realizamos $K\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 19 \\ 2 \end{pmatrix}$ tenemos el siguiente sistema de escuaciones:

$$k_{1,1} = 19$$

$$k_{2,1} = 2$$

   Para encontrar los otros coeficientes, sustituimos estos valores en la matriz K, y como sabemos que el par **AU** se cifra con el par **MI**, lo que quiere decir que al aplicarle K al vector $(0, 20)$, este se transforma en $(12, 8)$, es decir:

$$\begin{pmatrix} 19 & k_{1,2} \\ 2 & k_{2,2} \end{pmatrix}\begin{pmatrix} 0 \\ 20 \end{pmatrix} = \begin{pmatrix} 12 \\ 28 \end{pmatrix}$$

   Lo que nos genera el siguiente sistema de congruencias, que resulta ser muy sencillo:

$$20k_{1,2} \cong 12 (\text{mod } 26)$$

$$20k_{2,2} \cong 8 (\text{mod } 26)$$

   Donde notamos que las soluciones son $k_{1,2} = 11$ y $k_{2,2} = 3$, así hemos encontrado todos los coeficientes de nuestra matriz K de cifrado, la cuál resulta ser:

$$K = \begin{pmatrix} 19 & 11 \\ 2 & 3 \end{pmatrix}$$

   Ahora para encontrar la matriz de descifrado, buscamos la matriz inversa Q de K, para eso al calcular el determinante de K hacemos:

$$\|k\| = 3(19) - 2(11) = 57 - 22 = 35 (\text{mod } 26) = 9$$

   Ahora con el inverso multiplicativo de 9 módulo 26, que es 3, lo usamos para calcular Q que es igual a multiplicar el inverso multiplicativo del determinante de K con adjunta de la matriz traspuesta de K, lo que resulta:

$$K^{-1} = Q = 3\begin{pmatrix} 3 & 15 \\ 24 & 19 \end{pmatrix} = \begin{pmatrix} 9 & 45 \\ 72 & 57 \end{pmatrix} (\text{mod } 26) = \begin{pmatrix} 9 & 19 \\ 20 & 5 \end{pmatrix}$$

   Donde el inverso aditivo módulo 26 de 11 es 15 ya que $11 + 15 = 26 (\text{mod } 26) = 0$, y el inverso aditivo módulo 26 de 2 es 24, por que $2 + 24 = 26 (\text{mod } 26) = 0$, por lo tanto la matriz de descifrado es:

$$Q = \begin{pmatrix} 9 & 19 \\ 20 & 5 \end{pmatrix}$$

Ya con la matriz de cesifrado, la usamos para descifrar el mensaje, que resulta ser el siguiente:
EL SABADO FUIMOS A UNA BODA A MI NO ME GUSTAN LAS BODAS PERO A MI TIA CHOFI LE ENCANTAN DURANTE VARIOS DIAS SE ARREGLA SE ACICALA Y SE VISTE CON PLUMAS PIELES PIEDRAS Y GUANTES PERO HAY ALGO QUE SIEMPRE ME QUITA LA RESPIRACION SU PEINADO Y ESCUANDO HAY UNA BODA PRIMERA COMUNION QUINCE O FUNERAL MI TIA CHOFI HACE UNA CITA EN EL SALON DE BELLEZA ELODI