

Primer tarea

Manuel Díaz Díaz, Gerardo R. L.H. Canek Aguilar.

September 13, 2022

- 1) Explique brevemente porque en \mathbb{Z}_n dados $a \cong b \pmod{n}$ y $c \cong d \pmod{n}$, se tiene que $ac \cong bd \pmod{n}$.
- 2) Resuelva el siguiente sistema de congruencia en caso de tener solución, en caso contrario justifique por que no tiene solución.

$$x \cong 25 \pmod{35}$$

$$x \cong 15 \pmod{65}$$

$$x \cong 10 \pmod{15}$$

$$x \cong 35 \pmod{55}$$

$$x \cong 55 \pmod{85}$$

- 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 $a=0, \dots, z=25$, 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 RXTPFKQRSQ NPRQFMKRQ QRIRST-
FVLQ QF KM TLJA FRK 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 RK-
TPR ILQ FKTRPLSSFMKRQ RKTTPR ILQ NPMTRFKLQ Q ER IMQ SMV(LIBL,RTL,CLJJL,ERITL
Y MJFSPMK) Y RI PRSRNTMP LSREMQ. IMQ LJFKMLSFEMQ SMJNLPTFEM RKTTPR
TMELQ ILQ NPMTRFKLQ Q OUR QR UKRK L LSREMQ NRPJLKRSRK SMKQTLKTRQ IM
OUR FKEFSL OUR RQTMQ LJFKMLSFEMQ QMK RQRKSFLIRQ NLPL IL UKFMK NPRS-
FQL LI PRSRNTMP. IMQ SMJNIRGMQ PAE NLPL SLEL VLPFLTR SMK RI PRSRNTMP
QR UTFIFZLPMK NLP FERKTFBFSLP IMQ LJFKMLSFEMQ FKVMIUSPLEMQ RK IL FK-
TRPLSSFMK 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 PRSMKMS-
 FJFRKTM PREUSFEM NMP NLPTR ER IMQ LKTF SURPNMQ KRUTPLIFZLKTRQ. KURQTPMQ
 PRQUITLEMQ QUCUFRPRK OUR ILQ NPRQFMKRQ QRIRSTFVLQ QMK FKEUSFELQ NMP
 IL VLSUKLSFMK JLQFVL RK TMEM RI JUKEM Y NMP NRPQFQTRKSFL ER FKBRSSFMQ
 PRSUPPRKTRQ RK FKEFVFEUMQ FKJUKMERNPFJFEMQ, OUR KM RIFJFKLPMK IL FK-
 BRSSFMK Y LSLALPMK BLSFIFTLKEM IL QRIRSSFMK ER VFPUQ SUYLQ SLPLSTRPFQTF-
 SLQ QMK EFBRPRKTRQ L IMQ SMV LKTRPFMPRQ, JRKMQLNLTMCRKMQ NRPM SMK
 JLYMP TPLKJFQFAFIFELE.

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

Aplice 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.

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

XIM	QNP	LBV	FPC	MWI	ZLH	MAA	IVI	QLY	SIB
DES	IZM	UET	BPB	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	OVV	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	

- 4) El siguiente mensaje fue cifrado con el algoritmo de Hill poniendo en correspondencia $a=0, \dots, z=25$, sin ñ, ni puntos ortográficos.
- a) Encuentre la matriz de cifrado y proporcione solo 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 sabado 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