Primer tarea.

Manuel Díaz Díaz,Gerardo Rubén López Hernández

8 de marzo de 2020

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

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

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

   a)

$$\begin{aligned} x &\cong 10 \quad mod(65) \\ x &\cong 25 \quad mod(85) \\ x &\cong 35 \quad mod(70) \\ x &\cong 15 \quad mod(35) \end{aligned}$$

   b)

$$\begin{aligned} x &\cong 15 \quad mod(35) \\ x &\cong 10 \quad mod(65) \\ x &\cong 25 \quad mod(85) \\ x &\cong 15 \quad mod(145) \end{aligned}$$

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 EQDNSMBQJADJ 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 KOLRJFO 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, GORNTOR IMR NMIDJIAJUOSDEMR, ITOBM IMR EDAQJGMR OL UIMPTOR EMKM CDII Y JRD. OR KTY DKNMQSJLSO SOLOQ OL ETOLSJ PTO RML TL BQTNM Y

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

a) Hacer análisis de frecuencias.

b) Dar la clave de cifrado.

c) Dar la regla de descifrado.

d) Descifrar el mensaje (es decir poner el texto completo descifrado).

5) Dado el siguiente mensaje cifrado con Vinage.

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

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

b) Dar la clave de cifrado.

c) Descifrar el mensaje.

6) Dado el siguiente mensaje cifrado con Hill del cual se tiene que:IQ SU NF WI FE IY IK CC KO IG UV proviene de:Como ho ye nd ia es mu yc om un

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

JX ZL YB RR GI IQ YR PN FE CN RR EJ GH NB UQ SO KY ZH OI NN LP GC HV SC PN EY JT FE IK EM DM US OT MU YB PN RZ GO UR AN SF OU AP CW OT MC CO VD BU AN RT GO WD KJ EZ NH RL YB EZ IK RT SU KY XI ME EW UI PF CN EY YG SG QK EZ RT PT YM

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

b) Calcular la matriz inversa paso a paso.

c) Descifrar el mensaje.