# Primer Tarea de Criptografía y Seguridad.

Manuel Díaz Díaz, José Canek García Aguilar y Gerardo Rubén López Hernández

24 de febrero de 2019

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

2) Resolver las siguiente congruencias y en caso de no tener solución decir porque no tiene solución:

   a) $111x \cong 75 \mod(321)$.

   b) $7x \cong 5 \mod(243)$.

   c) $15x \cong 11 \mod(625)$.

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

$$\begin{aligned} x &\cong 32 \mod(83) \\ x &\cong 70 \mod(110) \\ x &\cong 30 \mod(137) \end{aligned}$$

4) Descifrar el siguiente mensaje el cual se sabe que esta 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.

5) Decifrar el siguiente mensaje que fue encriptado con Vigenere, recuerda 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

6) Decifrar el siguiente mensaje que fue encriptado con Hill, y se tiene la siguiente información: "vectorial real sobre elcampo 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.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 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