Practico 1 de Criptografia-2005

1): Encripte LLEGARE A ROMA EN DOS DIAS con el Cesar shift.

2): Encuentra un mensaje que dice:
KPYP NHZL HZHU AHML JVUZ BZAY VWHZ
y sospecha que es un shift con alguna clave. Desencriptelo. (asuma todas las letras menos la $\tilde{n}$).

3): Encuentra un texto que dice DSRYLSLNSETUEOPAO.
Sospecha que ha sido usado solo un cifer de transposición muy simple, pero no sabe cual. Descifre el mensaje.

4): Encripte ATACAR AL AMANECER usando:
a) Cesar Shift.
b) Algun codigo monoalfabetico de su invencion.
Observar las repeticiones en a) y en b).
c) Un codigo Vigenere con palabra clave MAGICO.
Observar las repeticiones en la primera y septima letra.
d) Un codigo Vigenere con palabra clave TIRABUZON.
e) Un metodo playfair con palabra clave MAGICO
f) El metodo ADFGVX con palabras clave TIRABUZON-MAGICO.
g) El metodo Hill con alguna matriz de su invencion.

5): Ud. intercepta un mensaje que dice:
ECABINANKGGLQICAUFMNIN
Luego, Ud. sabe que fue encriptdo usando un metodo Playfair con matriz 5 por 5, y palabra cable MONARQUIA. Desencripte el mensaje.

6): Ud. intercepta un mensaje escrito por alguien que Ud. sabe esta usando un codigo Hill 3×3. El mensaje interceptado es:
XFW SRG YAY XTM LKD UZI CHI SXK ÑDE RIS ÑKL LBU NTB EJB OBB UTO AUY
Un colaborador suyo encuentra en el lugar de transmision la primera parte del mensaje, que comienza:
NOS DESCUBRIE
?Que dice el resto del mensaje?

7): a) Escriba un programa que tome un texto ASCII y le haga un Cesar Shift.
b) Modifique el algoritmo de a) para que ahora el shift sea dependiente de una clave y cambiante de letra a letra. (Encriptamiento Vigenere). (Recordar que la clave puede ser de longitud arbitraria, y si el mensaje es mas largo que la clave, debe repetirse la clave desde el principio).

8): Escriba un programa que cuente las frecuencias de las letras en un texto dado. Corra el programa con diversos textos en castellano, y elabore una tabla de distribucion de frecuencias de las letras en castellano.

9): Se intercepta el siguiente mensaje, que sospecha que ha sido encriptado con Vigenere:
MUCY UWMF TNLN PVXN IHHL QJRU IWBW DZJE QLAI FMNM IBNJ TJJS UJVI CGLJ LJVI BGCB VZNY HWAB CWTA GSWB GDWU ESAB TJZO TJAB XNKI PDVJ AVHN XWVQ WYEU CLNB ADLX JVJT LNJO TDXT ONGY GSUF ABXJ PFDT IAEI TXND BROU BWWU MHJO THJS IZNY HWYV MMTH PHAP DNVB PJBV AYHN TFLJ IUBX PVNT LNUY WSLF ZBXO CMBP MWFU HSMF TXLG XKVP AHGI TFOP ZVTC CVRW QMNU AQYM IWMY PDJS MJEC OSLJ WWWY JFJH ZJGI UWWT QETX TLJO YDXM TDYS QVXL SAJE MUFY HWWU ZJGN T.
Desencriptelo. (asuma idioma castellano sin $\tilde{n}$) (nota: conviene haber hecho el ejercicio anterior antes)

10): Escribir un programa que encripte usando el metodo ADFGVX, usando primero la expansión-substitución, luego la permutación, y finalmente una nueva substitución-compresión. Haga que el programa pida una clave, la cual debe ser la forma nmK, donde n y m son numeros. n se usa para leer los primeros n caracteres de la clave K. Estos se rellenan en una matriz 6×6, eliminando letras repetidas, y luego se completa el resto del alfabeto para rellenar la matriz. Luego, transponga la matriz. Esta sera su matriz para la expansion-substitucion. Luego, se usa m para leer los siguientes m caracteres de K, esto se usa como la clave para la permutacion. Finalmente, se usan los caracteres finales de K para realizar, en forma similar con la primera matriz, una nueva matriz que se usara para la substitucion de comprension.

b) Modifique el sistema para usar ahora, digamos un metodo ADFGVXC, y escriba matrices 7×7, usando los siguientes caracteres extras: Ñ , . ; : ( ) \$ % + = ! ?