AUTOESTUDIO CRIPTOGRAFÍA CLÁSICA

Curso 15_16. Fundamentos de Seguridad

"SABER ROMPER MEDIDAS DE SEGURIDAD NO HACEN QUE SEAS HACKER AL IGUAL QUE SABER HACER UN PUENTE EN UN COCHE NO TE CONVIERTE EN UN INGENIERO DE AUTOMOCIÓN"
Eric Raymond. http://es.wikipedia.org/wiki/Eric_S._Raymond.

Todas las tareas de la práctica pueden ser resueltas sin necesidad de utilizar un software, no obstante si queréis hacer alguna comprobación se puede utilizar software quese puede descargar en esta dirección http://www.criptored.upm.es/paginas/software.htm

Tarea 1. ¿Cómo se cifra el siguiente mensaje latino M = AQUILA NON CAPIT MUSCAS, si se utiliza una escítala de tres caras y se pueden escribir 8 caracteres (el blanco cuenta)? ¿Cómo se descifra el criptograma siguiente C = AE NMHIIOMNRUIRSSE STME, si se utiliza la misma escítala?

Tarea 2. Cifra con el valor $N_F = 6$ el mensaje M = EL COMPORTAMIENTO ES UN ESPEJO EN EL QUE CADA UNO MUESTRA SU IMAGEN utilizando el mecanismo explicado en clase para transposición por filas.

Tarea 3. Descifra el siguiente criptograma de cifra por columnas C = SROTAE IESOSL BSDS SOUUINIM SLSOEICT THMSAAIA PMSDNGRO y clave Nc = 8, utilizando el mecanismo explicado en clase para la transposición por columnas.

Tarea 4.

a. Se sabe que el siguiente texto cifrado C = **XFGJ**W VZJXJ **XFGJ**P TVZJX J**XFGJ** DVZJR TXJ**XF GJ**PTV ZJRTX J**XFGJ** MJFVZ NJPAJ WIFIJ WT**XFG J**W, se ha obtenido por el método de sustitución "desplazados puros". Como interpretarías que la cadena XFGJ se repita 6 veces?.

Tarea 5. Se recibe el criptograma que se indica:

DCONU VDOFV NMOCM WNPOP UVNWP WDWVN VDMWN WMOIO VNUWP ONWUC IHOVN VNDCQ VPULV XCQVC BDOMC LDWPM WNWMO IOVNU WPVND CBLCM UOMCZ NCALC PVQVC LOPUW UVDVP

Sabemos que ha sido cifrado mediante una sustitución monoalfabeto afín trabajando en módulo 27, es decir, en español y sólo letras mayúsculas.

a. Utilizando las expresiones algebraicas, encuentra el algoritmo de cifra, es decir los valores de las constantes a y b, sabiendo que las letras más frecuentes en el criptograma y su frecuencia relativa son: V = 13,6%, O = 10,39%, C = 10, 39%.

b. Escribe la ecuación de descifrado

c. Descifra los primeros 14 caracteres

Tarea 6. El siguiente criptograma ha sido cifrado con el sistema de cifra Vigenère. Algunos n-gramas repetidos en el criptograma se muestran con subrayados, negritas.

VGJSVJVANSIUEOVIFOUUPUDAHOHMMNKUVBJAIJQEEHQEDEAEKSYOUWJVVG
EEKIQDRQXNMBJCREJQMSCEEWJUEOLAHJLHRRNCGZXRJDROHDAEKDTAXSVT
VSVLMUJRUSTLRAJRCOYOJHDNGAKRVZJCGBXCZOVPGGNLU**SLAHSAUTWCA**J
DRAMBMIRZNDZXXATOYEJJLILOBUDOUAYWRADWJMVRQCVBZUVZJASJNLZIJE
KIJEETNRDOPEHSVSRRXQMSLODDPOPBXTZSVEKQXLVUQOHDMRZOBLCSEAJZ
NACU**DNRH**LOKWCAKNMEHOBOYOLEJZNCGAYAFWJMZGJHVANTZRXEESBTVQ
NSLD**DNRH**COJIQTRHUAEINCRNDNRXJRJWCATDVMZSTCJJIAKSTBGHZUVHQNV
BCRVINNVGCEPHNLRHTLVKJSP**OEEJOB**CMOVTGBXSCDJGJOMET**SLAHSAUTWC**
AKSYUKDBUTOYAPIXMRBMOVZLEKIXSVSVCRAQNGVJCZONLSDBQMSPATWJU
EOCAJRNMRGJVZZTOKOHECZJSVHNNLWJFVZQZHDAQMSQBR**OEEJOB**URPDEC
WCA

a. Las distancias entre las repeticiones son 56, 76, 84, 132, 136, 292. Indica a qué n-gramas corresponde rellenado la tabla siguiente

b. ¿Cuál de estas cinco claves habrá cifrado el mensaje M? Justifica tu respuesta. K_1 = AZUL, K_2 = ROJA, K_3 = AMARILLA, K_4 = VERDE, K_5 = MARRON.

c. Descifre sólo los caracteres LAHSAUTWCA en su primera aparición en el criptograma. Note que la aparición de esa palabra está en la posición 162

Tarea 7. Un cifrado de Hill ha utilizado una de estas claves simbólicas K1 = MILITANTE, K2 = CALAVERAS o K3 = AMATISTAS trabajando en el cuerpo de las letras mayúsculas.

Recuerde que con claves simbólicas la clave escrita de izquierda a derecha da lugar a sus elementos. Por ejemplo, para la clave K1 se tiene:

k11 = M, k12 = I, k13 = L, k21 = I, k22 = T, k23 = A, k31 = N, k32 = T, k33 = E

A. ¿Cuál podría ser la clave usada en la cifra y por qué descarta a las demás?

b. Si el criptograma de la cifra es

ÑLUDRAOXLQITMCHYHNSBVNRADPETIJPIJEFVLWZFIRTKHTHVKXDGVCJSDBRA
SXTURRHZQQYUDRANFVPZNVZJHBVFTWKOLABAOBEZCKFHWRRREYBXVNWH
ZKMMDKAWÑETCVMENTGVHVBDPECQZQBVSYHEYBXVNWHZKMMSBI

Utilizando operaciones matriciales se pide descifrar los nueve primeros caracteres del criptograma. Se deben escribir las operaciones en la solución

Tarea 8. (1,5 PUNTOS) Busca una variante del Cifrado de Vigenère que se denomina Autoclave o S**egundo Cifrado de** Vigenère y muestra con un ejemplo pequeño cómo se cifra y se descifra utilizando dicho cifrador.