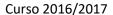


Universidad Carlos III de Madrid

Criptografía Clásica

CSI Curso 2016/2017





Ejercicios Criptografía Clásica.

(Obs: Considérese el alfabeto en castellano en mayúsculas de 27 caracteres).

- √1. Dada la función de cifrado E(m)=7m+3 Mod.27 se pide: ♣ /B 시... / ₹ %
 - a. Valores de las constantes de decimación y desplazamiento.
 - b. Cifrar el mensaje "TERCERA" 8/4/24/43 /4/24/3 I EUQEUD
 - c. Descifrar el mesnaje "DID ÑOE"

- 2. Dada la clave "LUCI" cifrar el siguiente mensaje mediante el método de Vigenere. M= "CAMINERO".
- 3. Dada la clave "PLUS" descifrar el siguiente mensaje sabiendo que fue cifrado mediante el método de Vigenere. C= "LSAW COMW".
- 4. Dada la clave "ALA" descifrar el siguiente mensaje sabiendo que fue cifrado mediante el método de Vigenere con Autoclave. C= "EDVI KVQG".
- 5. Dada la clave "MARTES" cifrar el siguiente mensaje mediante el método de Playfair. M= "FALSO PUENTE".
- 6. Dada la clave "MARTES" descifrar el siguiente mensaje sabiendo que fue cifrado mediante el método de Playfair. C= "FOMUMB ZFTERZ".
- 7. Dada la matriz clave $K = \begin{bmatrix} 3 & 2 \\ 4 & 6 \end{bmatrix}$ se pide:
 - a. Valorar si la matriz reúne las condiciones para utilizarse como clave en un método de sustitución polígrafa de Hill.
 - b. Cifrar el mensaje M="RECORDAR" mediante el método de Hill.
- 8. Dada la matriz clave $K = \begin{bmatrix} 7 & 6 \\ 3 & 11 \end{bmatrix}$

Se pide descifrar el mensaje C="J8D6 L4N3" sabiendo que el alfabeto utilizado es {A,...,Z}+{0,...,9}.

9. Habiendo utilizando la siguiente permutación KP= (642135) se pide descifrar el mensaje C= "OOEMTD/IACSLS EEOCSE"
6 4 24 3 3 44 243 5 K 42 43 5

METODOS SCLASI COSEEE = METODOS CLASICOS

```
CAMINERO = NUN PYZTW
             2) CAMI NERO
                       NUNP XX TW
                                                                                  OVWXO
CDEFGHIJKLHN®OPQRST
IJKLHNNOPQRSTUV®
                                                         COMW => VIGENERE
                                                                                                                               EFG HI
                                                                                                                                                                                                              NÃOPA
                                                                                                                                                                                                   3 (D O
                                                                                              MNNOPORS
                                                                                           TUVO PARST
                                                                                                    Mirande toda afforta como esta pero la clava la propia
             4) FDVI KVQG.
                            A LAE SVE R
                           ESVERAND
                                                                                           ES VERANO
wither drugers
when drugers
como dace.

5) MARTES
                                                                                                                                                        & Opverto restich
                                                                                                                                                                                       Espejo >
                                                                                                                                MARTE
                                                                                                                                                                                                   BEGF Paz Famrz
                                                                                                                               SBCDF
                      FALSO PUENTEX
                                                                                                                               GH IJKL
                    BE GF PQ CF QH RT
                                                                                                                                  NO P Q U
                                                                                                                                  V M X Y Z
                    a el opuesto en la vertical
                                                                                                                                                                                                4-1. / opento vertical es en il
                         en el avadro que forman la des
                6) MARTE
                                                                                                                                                                                            MARTE
                                                                                                                                                                                            SBCDF
                               FOMUMB EFTERE => BUENA SUFRTE X
                                                                                                                                                                                                GHINGL
                                                                                                                                                                                              NROP Q U
                                                                                                                                                                                                V w x Y 🔁
             7) k= (3 8) lundiste 1K1+0=del(K)
                             RE CO RD AR = 105QGJJA
                    (C1)= (3?)(18)= (1) mod 27 (C3)= (3?)(2)= (6+20) mod 27
                     \binom{C_5}{G} = \binom{18}{3} = \binom{
```

$$K^{-1} = \frac{1}{\det(k)} K^{-1} = \frac{1}{59} \binom{11-6}{-3-7} \text{ mod } 37 = 59^{-1} \binom{11-6}{-3-7} \text{ mod } 37 = 32 \binom{11-6}{-3-7} \text{ M}$$

$$\binom{7-6}{3-11} \binom{11-6}{3} \pmod{37} \pmod{37}$$

$$\binom{7-6}{3-11} \binom{11-6}{3} \pmod{37} \pmod{37} \pmod{37}$$

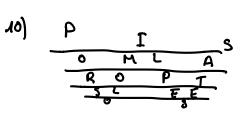
$$M = 32 \begin{pmatrix} 14 - 6 \\ -3 & 7 \end{pmatrix} \begin{pmatrix} 3 \\ 33 \end{pmatrix} = \begin{pmatrix} 1 \\ -6 \end{pmatrix} \begin{pmatrix} 14 \\ 3 \end{pmatrix} \begin{pmatrix} 14 \\ -5 \end{pmatrix} \begin{pmatrix} 11 \\ 34 \end{pmatrix} = \begin{pmatrix} 14 \\ 5 \end{pmatrix} \begin{pmatrix} 29 \\ 5 \end{pmatrix} \begin{pmatrix} 14 \\ 5$$



10. Habiendo utilizando una transposición con 5 filas de recorrido en zig-zag descifre el siguiente criptograma: C="PISOML AROPTS LEEOS"

Secale To a SCEO ERT

11. Cifre mediante una transposición columnar de 4 columnas el siguiente texto M="FIESTA NACIONAL".



PORSOLOMIL PESETAS

= FTCA IAILENOX SANX