Introducción a la Criptología

Problemas de Criptología - Hoja 1

Curso 07-08

1 **Claves débiles y claves de poca calidad.** Estudia las claves débiles y las claves de poca calidad de los siguientes cifrados: el cifrado de atbash, el escitalo, el cifrado de César, la rueda de Alberti, el cifrado de Vigenère, el cifrado de Wheatstone-Playfair, el cifrado de Vernam y el cifrado ADFGVX.

2 **Cifrados y ataques.** Establece para los criptosistemas del problema anterior cómo les afectan los distintos tipos de ataque.

3 **El escitalo.** El siguiente mensaje ha sido codificado con un escitalo de 9 caracteres:

LOVORPOAEANEPEASRNRERASRYATESDRFAU

DELAAAASTISILDPLAIR−GGEOSBLI−IORBOIPG−

Descifra el mensaje (es una frase de Séneca). El signo − indica un espacio en blanco.

4 **Criptoanálisis del escitalo.** Elabora un criptoanálisis para el escitalo. Prueba el criptoanálisis tratando de descifrar el siguiente mensaje.

NLDSQANGUOAIUEAANGSAESTNCRISETUAAAN

MSARSSDEOTAA−EONAUSC−HNTSDIO−AAUIIGN

El signo − indica un espacio en blanco.

5 **Cifrado de César.** Consideremos el alfabeto español {A,...,Ñ,...,Z} de 27 letras.

(a) Cifra la siguiente frase de Jardiel Poncela con el cifrado de César:

El amor es una comedia en un acto: el sexual.

(b) El mensaje de más abajo se ha cifrado con el cifrado de César. Descífralo.

HVWXSLGHCKXODPDKXODPDVREUDUHDÑOHP

WHÑRVXPLFRVHVWSLGRVVRQÑRVKROEUHV

6 **Cifrado de Vigenère.** Codifica el mensaje de abajo con el cifrado de Vigenère usando la letra p como letra inicial.

La ignorancia y el error son manantiales de mal humor.

7 **Cifrado Wheatstone-Playfair.** Codifica, usando el cifrado de Wheatstone-Playfair, el mensaje *Dime y lo olvido, enséñame y lo recuerdo, involúcrame y lo aprendo* (Cita de Benjamín Franklin).

8 **Cifrado ADFGVX.** Codificar el mensaje *Aprende o muere* con el cifrado ADVGVX usando *panoli* como clave para la transposición.