Ejercicios: Criptografía clásica

2.1) La criptografía clásica abarca desde tiempos inmemoriales hasta la mitad del siglo XX. El punto de inflexión en la clasificación de los criptosistemas como clásicos o modernos lo marcan tres hechos relevantes acaecidos en 1948, 1974 y 1976. Explica en qué consistieron.

2.2) Un criptoanalista afirma que el criptograma

c=ALXB TH HKRRRRRYV

ha sido obtenido cifrando mediante un sistema de sustitución simple un mensaje escrito en castellano. ¿Es cierto?

2.3) Cifra tu nombre y apellidos utilizando un método de sustitución simple en el que se aplica la transformación $c_i=E_k(m_i)=(11m_i+2) \bmod 28$ al alfabeto

A={ _ABCDEFGHIJKLMNÑOPQRSTUVWXYZ}

Obtén la transformación de descifrado D_k.

2.4) Repite el ejercicio anterior con el alfabeto

A={ ABCDEFGHIJKLMNÑOPQRSTUVWXYZ}

utilizando módulo 27.

2.5) Un equipo de delincuentes informáticos ha interceptado un mensaje cifrado que se transmite entre dos sucursales bancarias, tras meses de intento. El mensaje contiene la clave de acceso a las bases de datos para el día. Se sabe que el sistema criptográfico que utilizan es de sustitución simple y que a las letras C e I del texto en claro le corresponden C y Z respectivamente en el criptograma. El alfabeto utilizado es

A={ ABCDEFGHIJKLMNÑOPQRSTUVWXYZ}

a) ¿Pueden obtener la clave utilizada con estos datos?

b) Si la clave es cambiada y sólo se conoce que la letra M del texto en claro se corresponde con la M del texto cifrado, ¿pueden obtener la clave?

2.6) Consideremos el alfabeto

A={ _ABCDEFGHIJKLMNÑOPQRSTUVWXYZ}

Mediante un método de sustitución simple en el que

$c_i=3m_i+8 \bmod 28$

a) Obtén la tabla de sustitución (cifrado-descifrado).

b) Cifra el mensaje m=ESTA_NOCHE_FUEGO.

c) Sin hacer uso del apartado a), descifra el criptograma

c=CKIFQVHSVHN_RNVI_L

d) Realiza un estudio sobre las frecuencias de aparición de letras en el texto en claro del apartado b) y del criptograma en el apartado c) e intenta obtener la clave.

2.7) Se desea cifrar el mensaje

"ES EVIDENTE QUE UN GOBIERNO NO PUEDE DECIR LO QUE PIENSA A LOS MERCADOS FINANCIEROS, PERO NO ES MENOS OBVIO QUE RESULTA SUICIDA MANTENER UNA DIVISA CONTRA VIENTO Y MAREA. APUESTO POR TOMAR UNA DECISIÓN VALIENTE, AUNQUE ARRIESGADA, QUE NO ES OTRA QUE DEVALUAR SIN ESPERAR A QUE LOS MERCADOS OBLIGUEN A ELLO, SIN AGUARDAR POSTERIORES CONDICIONAMIENTOS"

mediante un sistema mixto: las consonantes se cifrarán mediante un sistema de sustitución simple y las vocales mediante uno homofónico.

a) Obtén las frecuencias de aparición de las vocales en el texto en claro.
b) Describe el método que utilizarías para que las frecuencias obtenidas en el apartado anterior no sean significativas en el criptograma.

2.8) Si se pretende utilizar el método Vigenère para cifrar un mensaje, ¿qué palabra clave resulta más conveniente?

TE, CAFETÍN, POLEO o MANZANILLA

2.9) El siguiente criptograma se ha cifrado utilizando el método Vigenère.

PL ÑGTMCG OIY RPL KSE

Se sabe que la clave está guardada en un cajón que contiene las siguientes palabras

CAJA, LOZA, MAYO, MOTO, CALA, META, LAZO, MOYA

Averigua cuál es la clave utilizada y obtén el texto en claro.

2.10) Utilizando el código ASCII binario cifra el mensaje m=SAL mediante el método Vernam. La clave utilizada es YES.

2.11) Sabiendo que se ha usado el método Vernam para aplicar un doble cifrado con claves k_1=10011100 y k_2=00111100, ¿cuál es el texto en claro del criptograma c=00001111?

2.12) En el cifrado de Vernam con clave binaria aleatoria, ¿que tiene que ocurrir para que el criptograma obtenido al cifrar sea una serie de unos binarios?