Hoja de Problemas 1 de Criptografía

1. Estudiar la cifrador de Polybios.
2. Estudiar la cifrador de Playfair.
3. Estudiar el cifrado ADFGVX.
4. Estudiar la arquitectura OSI de seguridad y la recomendación X.800.
5. Dado un cifrado afín $y = a \cdot x + b$ en Z_m demostrar que este constituye un criptosistema si $mcd(a, m) = 1$.
6. Demuestra que un entero decimal es divisible por tres si la suma de los dígitos es divisible por 3.
7. Demuestra el teorema de Lamé: Si $a, b \in N$, $a > b$ y el Algoritmo de Euclides toma $n + 1$ iteraciones en encontrar el $mcd(a, b)$, entonces $n < log_g b$ con $g = (1 + \sqrt{5})/2$
8. Usar el algoritmo de Euclides para calcular $d = mcd(a, b)$ y encontrar u y v tales que $d = au + bv$ (teorema de Bezout), en cada uno de los siguientes casos:
   a) $a = 63, \quad b = 28$
   b) $a = 56, \quad b = 27$
   c) $a = 721, \quad b = 488$
9. Calcula el valor exacto del número de llaves cuando el método de Hill está en Z_p donde p es un número primo y $n = 2$.
10. Resuelve las siguiente congruencias:
    a) $3x \equiv 4 \bmod 7$
    b) $3x \equiv 4 \bmod 12$
    c) $9x \equiv 12 \bmod 21$
    d) $27x \equiv 25 \bmod 256$
11. Averigua la llave utilizada en un método afín cuando tenemos que el texto original es “3241” y el texto cifrado es “1203” en Z_6.

12. ¿Se ha usado el Hill con tamaño de clave $n = 2$ si se ha detectado el texto original "1323" y el texto cifrado "0121" en Z_4?

13. Si se utiliza la siguiente clave para cifrar mediante el método de Hill:

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix},$$

¿Se podría afirmar que tenemos un criptosistema de Hill en Z_{26}? ¿Cuál sería la inversa de esta matriz en Z_{26}?

14. Si se utiliza la siguiente clave para cifrar mediante el método de Hill:

$$\begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix},$$

¿Se podría afirmar que tenemos un criptosistema de Hill en Z_{26}? ¿Cuál sería la inversa de esta matriz en Z_{26}?

15. Encuentra varios ejemplos de funciones de cifrado por transposición y substitución que no sean criptosistemas.

16. Estudiar los registros de desplazamiento retroalimentados lineales y no lineales para generación de secuencias cifrantes de claves. Como ayuda podeis leere el capítulo 6 del libro Handbook of Applied Cryptography Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone (http://www.cacr.math.uwaterloo.ca/hac/).

17. Demuestra que si $D_K(E_K(x)) = x$ con $x \in P$ entonces $E(x_i) \neq E(x_j)$ para $x_i \neq x_j$.

18. Construye un árbol jerárquico que enlace los siguiente términos: cifrado por bloques, criptoanálisis, criptografía, criptología, llave privada, llave pública. cifrado de flujo.

19. Demuestra que el $mcd(a, b) = mcd(b, a \, mod \, b)$, para $a > b$.

20. Utiliza el algoritmo de Euclides para calcular el máximo común divisor de

a) 7469 y 2464

b) 2689 y 4001

21. Calcula los parámetros u y v de $u\ r_0 + v\ r_1 = mcd(r_0, r_1)$ en el siguiente ejemplo $r_0 = 31$ y $r_1 = 7$.

22. Calcula los inversos en Z_{27} de $a = 7$ y $a = 9$. Verifica los valores.

23. Sea $e_1(x) = a_1 * x + b_1$ y $e_2(x) = a_2 * x + b_2$ en Z_m. Determina los valores de los parámetros $a, b \in Z_m$ para $e(x) = a * x + b = e_1(e_2(x))$. ¿Cuál es tamaño del espacio de llaves de $e(x)$?

24. Calcula $\phi(m)$ cuando $m = p \cdot q$ donde p y q son primos. Demuestra que si $m = p \cdot q$ donde p y q son primos, entonces $\phi(m) = \phi(p)\phi(q)$

25. Utilizando la tabla de frecuencias para los 26 caracteres del inglés adjunta en la primera práctica de la asignatura, descifrar el siguiente texto cifrado por un método afín:

```
FMXVEDKAPHFERBNDKRXRSREFMORUDSDKDVSHWFEDK
APRKDLYEVLRHHRH
```

26. Utilizando la tabla de frecuencias para los caracteres del inglés y español adjunta en la primera práctica de la asignatura, calcular los índices de coincidencia para los dos idiomas.

27. Define producto de criptosistemas, explica razonadamente cuál es el motivo por el que se hace. Poner dos ejemplos de producto de criptosistemas, de tal forma que en uno de los ejemplos se incremente la fortaleza del criptosistema resultante y en el otro no. Analiza detalladamente y razona la fortaleza de los criptosistemas antes y después de ejecutar la multiplicación de los mismos.

28. Define índice de coincidencia y explica razonadamente como utilizar esta medida para calcular cada una e las componentes de la llave en un cifrado de Vigenere, cuando ya se conoce previamente la longitud de la clave.

29. Explica razonadamente el algoritmo extendido de Euclides. Deduce razonadamente todas las recurrencias que necesites para explicar este

algoritmo. Pon un ejemplo de la aplicación de este algoritmo. Explica y razona otro método que calcule lo mismo que el algoritmo extendido de Euclides.

30. Crea un pseudocódigo que de como resultado el inverso de un número en Z_m, que este basado en el algoritmo extendido de Euclides.

31. Test de *Kasiski*.

    a) Explica razonada y detalladamente en qué consiste el test de *Kasiski* y en qué está basado. ¿Cuál es el objetivo de su aplicación?

    b) Aplica el test de *Kasiski* al siguiente bloque cifrado mediante un criptosistema de *Vignère*.

    ```
    CHREEVOAHMAERATBIAXXWTNXBEEOPHBSBQMQEQERBW
    RVXUOAKXAOSXXWEAHBWGJMMQMNKGRFVGXWTRZXWIAK
    LXFPSKAUTEMNDCMGTSXMXBTUIADNGMGPSRELXNJELX
    VRVPRTULHDNQWTWDTYGBPHXTFALJHASVBFXNGLLCHR
    ZBWELEKMSJIKNBHWRJGNMGJSGLXFEYPHAGNRBIEQJT
    AMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQEBBI
    PEEWEVKAKOEWADREMXMTBHHCHRTKDNVRZCHRCLQOHP
    WQAIIWXNRMGWOIIFKEE
    ```

    Explica razonada y detalladamente cuál es el resultado de aplicar este test. *Nota: Utilícese la cadena "CHR".*

    c) ¿Existe otro método similar al test de *Kasiski*? ¿Hay algún método para descifrar el anterior bloque después de aplicar test de *Kasiski*? Explica y razona tus respuestas.

32. Dada la supuesta función de cifrado:

$$e_k(x) = ((x+1)(x-1)x) + ((x+1)^2 + 1) + b \bmod 10.$$

    Responde a las siguientes preguntas explicando por qué:

    a) Si $P = C = Z_{10}$ y $b \in Z_{10}$, ¿define esta función de cifrado un criptosistema?

b) Si $P = Z_4$, $C = Z_{10}$ y $b \in Z_{10}$, ¿define esta función de cifrado un criptosistema?

c) Si $P = Z_4$, ¿define esta función de cifrado un criptosistema con $C = Z_4$ para cualquier $b \in Z_{10}$?

33. Supongamos que tenemos el principio de texto original "FRIDAY...", que ha sido encriptado mediante un cifrado de Hill usando una clave de 2×2 en Z_{26}. El texto cifrado correspondiente es "PQCFKU...". Sabemos que los bloques para el cifrado por Hill se han obtenido situando los caracteres por columnas, así el primer bloque para cifrar con una clave de 2×2 es:

$$\begin{pmatrix} F & I \\ R & D \end{pmatrix}$$

a) Calcula la clave del cifrado.

b) Calcula la función de descifrado, comprobando que es correcta con los textos cifrado y original que se dan en el problema.

c) Haz una estimación del segundo bloque de texto plano y su correspondiente bloque cifrado.

Nota: Usa el siguiente alfabeto para la realización del problema:

```
(A= 0)(B= 1)(C= 2)(D= 3)(E= 4)(F= 5)(G= 6)(H= 7)(I= 8)
(J= 9)(K=10)(L=11)(M=12)(N=13)(O=14)(P=15)(Q=16)(R=17)
(S=18)(T=19)(U=20)(V=21)(W=22)(X=23)(Y=24)(Z=25)
```

34. Se utiliza la siguiente clave para cifrar mediante Hill en Z_{26} :

$$\begin{pmatrix} 10 & 5 & 12 \\ 3 & 14 & 21 \\ 8 & 9 & 11 \end{pmatrix}.$$

a) ¿Es un criptosistema? Demuestra y razona la respuesta.

b) Da un ejemplo de cifrado de Hill que no sea un criptosistema.

Supón ahora que en Z_6 tenemos el texto original '3241' que se transforma por un cifrado afín en '1203'.

a) ¿Cuáles son los valores de a y b?

b) ¿Es un criptosistema el cifrado afín que se ha utilizado? Si fuese un criptosistema calcula la transformación inversa.

Razona y demuestra todas las respuestas.

35. Se utiliza la siguiente clave para cifrar mediante Hill en Z_3 :

$$\begin{pmatrix} 1 & 5 & 7 \\ 1 & 3 & 4 \\ 8 & 2 & 2 \end{pmatrix}.$$

a) ¿Es un criptosistema? Demuestra y razona la respuesta.

Supón ahora que en Z_6 tenemos el texto original '3241' que se transforma por un cifrado afín en '1203'.

a) ¿Cuáles son los valores de a y b?

b) ¿Es un criptosistema el cifrado afín que se ha utilizado? Si fuese un criptosistema calcula la transformación inversa.

Razona y demuestra todas las respuestas.

36. Demostrar que $\sum_{i=0}^{i=m-1} P_i P_{i+l} = \sum_{i=0}^{i=m-1} P_i P_{i-l}$, donde las operaciones de suma y resta sobre los índices de las probabilidades se realizan en aritmética modular m.

37. Calcular el índice de coincidencia del inglés, castellano y un lenguaje aleatorio.