Hoja de Problemas 2 de Criptografía

1. Considera las variables estocásticas X, Y, Z que pueden tomar valores del conjunto $A_x = A_y = A_z = \{0, 1\}$. Además $P_x = \{p, 1-p\}$, $P_y = \{q, 1-q\}$ y X e Y son variables de procesos estocásticos independientes. El valor de Z se determina a partir de la relación

$$Z = X + Y \bmod 2$$

   a) Para un q y un p dado ¿Cuál es el valor de P_z?

   b) Supón que no conoces P_y pero sabes que $P_z = \{l, 1-l\}$. ¿Cuál es el valor de P_y?

2. Dos dados X e Y de 6 caras se lanzan

   a) ¿Cuál es la probabilidad de la suma de sus valores?

$$Z = X + Y$$

   b)

$$Z = |X - Y|$$

   ¿Cuál es P_z?

3. Considera un conjunto de mensajes $P = \{0, 1\}$ un conjunto de llaves $K = \{00, 01, 10, 11\}$ y conjunto de texto cifrado $C = \{00, 01, 10, 11\}$. La transformación del cifrado es la siguiente.

K	P=0	P=1
00	00	01
01	10	11
10	01	00
11	11	10

   Supóngase $P_p(0) = P_p(1) = 0{,}5$ y $P_k(K_i) = 0{,}25$.

   a) ¿Tiene este cifrado seguridad perfecta?

   b) Calcula la distancia de unicidad.

4. Considera un criptosistema con $P = \{a, b\}$, $K = \{k_1, k_2, k_3\}$ y $C = \{1, 2, 3\}$. Donde la matriz de cifrado es.

K	a	b
k_1	1	2
k_2	1	3
k_3	3	2

donde la distribución de probabilidad de las claves $P(k = k_1) = P(k = k_2) = 1/4, P(k = k_3) = 1/2$ y la distribución de probabilidad del texto original es $P(p = a) = 1/3$ y $P(p = b) = 2/3$. ¿Cuál es la probabilidad de obtener el mensaje si se conoce el texto cifrado?

5. Sea n un entero positivo. Se define el *Cuadrado Latino* de orden n como la matriz L de dimensión $n \times n$ compuesta por los enteros $1 \dots n$, de tal forma que cada uno de los n enteros aparece exactamente una sola vez en cada columna. Un ejemplo de orden 3 es:

$$\begin{matrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{matrix}$$

   Dado el el *Cuadrado Latino* de orden n, podemos definir el criptosistema asociado como $P = C = K = \{1 \dots n\}$ de tal forma que la regla de cifrado sea $e_i(j) = L_{ij}$. Probar explícitamente que este criptosistema cumple la condición de seguridad perfecta si la distribución de claves es $P_k(K) = 1/n$.

6. Demuestra que el cifrado Afín logra seguridad perfecta.

7. ¿Cuál es la distancia de unicidad del cifrado por desplazamiento?

8. ¿Cuál es la distancia de unicidad del cifrado por el método afín?

9. Tenemos que el espacio del texto original y cifrado es $P = C = (Z_{26})^2$ y usamos el método afín para cifrar. ¿Cuál es la distancia de unicidad?

10. Considera un conjunto de mensajes $P = \{0, 1\}$ con $P_p(0) = 1/3$, $P_p(1) = 2/3$, un conjunto de llaves $K = \{00, 01, 10, 11\}$ con $P_k(00) = P_k(01) = P_k(10) = 1/5$, $P_k(11) = 2/5$, y un conjunto de texto cifrado $C = \{00, 01, 10, 11\}$. La transformación del cifrado es la siguiente:

K_i |	P=0	P=1
00	00	01
01	10	11
10	01	00
11	11	10

a) Define y explica qué se entiende cuando se afirma que un criptosistema tiene seguridad perfecta.

b) Comprueba razonadamente si este criptosistema cumple la condición de seguridad perfecta. Calcula explícitamente las probabilidades $P_p(x|y)$ y $P_p(x)$.

c) Sabiendo que el número medio de llaves espúreas para un criptosistema con $|C| \neq |P|$ y $P_k(k) = 1/k$ cumple la siguiente relación:

$$\overline{S}_n \geq |K| \left(\frac{|P|^{1-R_L}}{|C|} \right)^n - 1,$$

deduce la distancia de unicidad, n_0 para este criptosistema, suponiendo que $P_k(00) = P_k(01) = P_k(10) = P_k(11) = 1/4$.

Nota: No utilizar el teorema del cifrado perfecto para comprobar la existencia o no de seguridad perfecta en este problema.

11. Describe el cifrado de Vernam (one-time-pad). Demuestra explícitamente que es un cifrado perfecto, sin aplicar el teorema del cifrado perfecto. Explica razonadamente si este cifrado se puede llevar a la práctica.

12. Calcula la distancia de unicidad para el método de cifrado afín, mediante la función de Euler, suponiendo que estamos en un alfabeto de m símbolos. Particularizar la expresión para el inglés (m=26), español (m=27) y un lenguaje aleatorio (m=100), suponiendo que la entropía de los dos lenguajes no aleatorios es 1,25. Explica cuál es el significado de los valores numéricos que has obtenido. (NOTA: Recuerda que la función de Euler es: $\phi(N) = \prod_{i=1}^{n} P_i^{(e_i-1)}(P_i - 1) = \prod_{i=1}^{n} P_i^{e_i} - P_i^{(e_i-1)}$, sabiendo que $N = \prod_{i=1}^{n} P_i^{e_i}$).

13. Considera un conjunto de mensajes $P = \{0, 1, 2\}$, un conjunto de llaves $K = \{01, 02, 11, 12, 21, 22\}$, y conjunto de texto cifrado $C = \{0, 1, 2\}$. La transformación del cifrado es la siguiente.

K	P=0	P=1	P=2
01	0	1	2
02	0	2	1
11	1	2	0
12	1	0	2
21	2	0	1
22	2	1	0

a) Explica razonadamente si esta transformación de cifrado define un criptosistema.

b) Define y explica que se entiende que un criptosistema tenga seguridad perfecta.

c) Comprueba razonadamente si este criptosistema cumple la condición de seguridad perfecta. Supóngase $P_k(K_i) = \frac{1}{6}$.

14. Explica detalladamente el concepto de llaves espúreas, poniendo un ejemplo. Sabiendo que el número medio de llaves espúreas para un criptosistema con $|C| \neq |P|$ y $P_k(k) = 1/k$ cumple la siguiente relación:

$$\overline{S}_n \geq |K| \left(\frac{|P|^{1-R_L}}{|C|} \right)^n - 1,$$

explica el concepto de distancia de unicidad y calcularla con esta expresión para las llaves espúreas. Supón que tenemos un lenguaje aleatorio con $|K| = 4$ (con $P_k(k) = 1/k$), $|P| = 2$ y $|C| = 4$. ¿Cuál es el significado del número que nos resulta para la distancia de unicidad?

15. Deduce las expresiones de $P_c(y)$ y $P_c(y|x)$ para el conjunto de de textos cifrados de un criptosistema utilizando el formalismo probabilístico. Define seguridad perfecta y razona cuál es su significado en relación a la seguridad de un criptosistema. Explicar y razonar qué relación deben cumplir $P_k(k)$ y $P_p(x)$ para que se cumpla la seguridad perfecta.

16. Considera un conjunto de mensajes $P = \{a, b\}$, con $P_p(a) = 1/4$ y $P_p(b) = 3/4$, un conjunto de llaves $K = \{k_1, k_2, k_3\}$ con $P_k(k_1) = 1/2$, $P_k(k_2) = P_k(k_3) = 1/4$, y un conjunto de texto cifrado $C = \{1, 2, 3, 4\}$. La transformación del cifrado es la siguiente:

	a	b
k_1	1	2
k_2	2	3
k_3	3	4

a) Define y explica qué se entiende cuando se afirma que un criptosistema tiene seguridad perfecta.

b) Comprueba razonadamente si este criptosistema cumple la condición de seguridad perfecta. Calcula explícitamente las probabilidades necesarias.

c) Transforma este criptosistema en otro que no cumpla la condición de seguridad perfecta si este la cumplía, o viceversa. Razona el resultado calculando explícitamente de nuevo las probabilidades necesarias para ello.

   Nota: No utilizar el teorema del cifrado perfecto para comprobar la existencia o no de seguridad perfecta en este problema.