Hoja de Problemas 3 de Criptografía: DES y AES

1. ¿Cual es el número total de sustituciones posibles si el tamaño del bloque es de n bits y nuestro alfabeto es m?

2. Demuestra que si aplicas la función de cifrado del DES sobre el texto cifrado con las llaves en orden inverso recuperas el texto original.

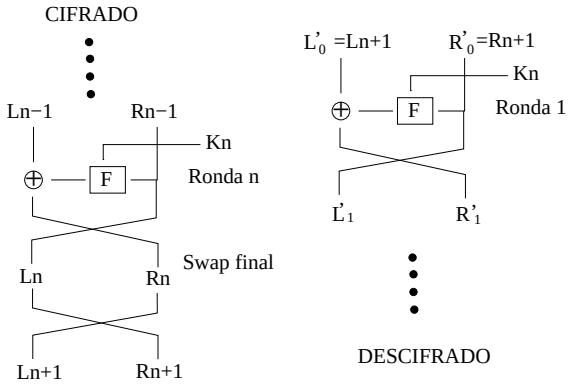
3. Que ventajas tiene el modo CTR sobre los otros modos de trabajo en el DES.

4. Cual es la diferencia en seguridad entre el DES doble y el triple.

5. Demuestra que
$$\overline{e_k(x)} = e_{\overline{k}}(\overline{x})$$

6. Explica detalladamente en qué consiste lo que se denomina *Attack in the midle* (ataque en el medio) para el DES doble. Nombra alguna de las posibles soluciones que existen

7. Según el diagrama de estructura Feistel para el DES de la figura, demuestra que $L'_1 = R_{n-1}$ y $R'_1 = L_{n-1}$.



8. ¿Puede el DES tener seguridad perfecta?

9. Calcula la distancia de unicidad en el ingles para el DES y DES doble. ¿Cuantos cifrados de bloques tenemos que hacer en cada caso para alcanzar la distancia de unicidad?

10. Explica qué son los modos de operación de un cifrado por bloques (tal como el DES o el AES), detallando cada uno de ellos. Explica también cuáles son las ventajas y desventajas de utilizar un modo de operación u otro.

11. DES:

    a) Dado un DES de únicamente 2 rondas demuestra que introduciendo las dos subclaves en orden contrario a como se introdujeron en el cifrado, se recupera el bloque en plano antes de cifrar.

    b) Dada la siguiente caja de sustitución S_1, calcula lo valores de las salidas de: $S_1(111111)$, $S_2(000000)$, y $S_1(100001)$.

14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

12. Respecto al algoritmo de encriptación DES:

    a) Demuestra explícitamente que $\overline{DES_k(x)} \oplus DES_{\overline{k}}(\overline{x}) = 0$. Para demostrarlo tienes que asumir una sola ronda del DES y demostrarlo solo para esta.

    b) Explica razonadamente en que consiste el ataque en el medio que se realiza sobre el DES.

13. Responde a las siguientes preguntas:

    a) Enumera y explica cuáles son los principios del diseño de las cajas S de sustitución del DES.

    b) Explica cómo se obtienen las cajas de sustitución del AES (la de cifrado y la de descifrado).

    c) Explica razonadamente por qué el DES no necesita tener una caja de sustitución para el descifrado, utilizando la misma que para el cifrado.

14. Explica detalladamente cuáles son los principios de diseño de la función F del DES, indicando y razonando qué beneficios producen en el

algoritmo. Comenta brevemente cuál es el esquema básico de esta función F. ¿Cómo probarías experimentalmente si la función F cumple los principios del diseño? Razona totas las contestaciones.

15. Demuestra explícitamente que $DES_k(x) \oplus \overline{DES_{\overline{k}}(\overline{x})} = 0$. Para demostrarlo tienes que asumir una sola ronda del DES y demostrarlo solo para esta.

16. Dados los modos de operación OFB y CFB del cifrado de bloques que se presentan en las figuras 1 y 2 respectivamente, dar una expresión para el cifrado y el descifrado de ambos modos de operación. Para ello lo único que hay que hacer es dar los valores de C_1 y C_j para el cifrado y P_1 y P_j para el descifrado de ambos modos, donde el indice $j = 2, ..., M$. Notar que las figuras para el descifrado no se presentan. Dejar los resultados en función de la función de cifrado genérica E_k, la función $S_s(X)$ que extrae los s bits más significativos de la un vector de bits X.

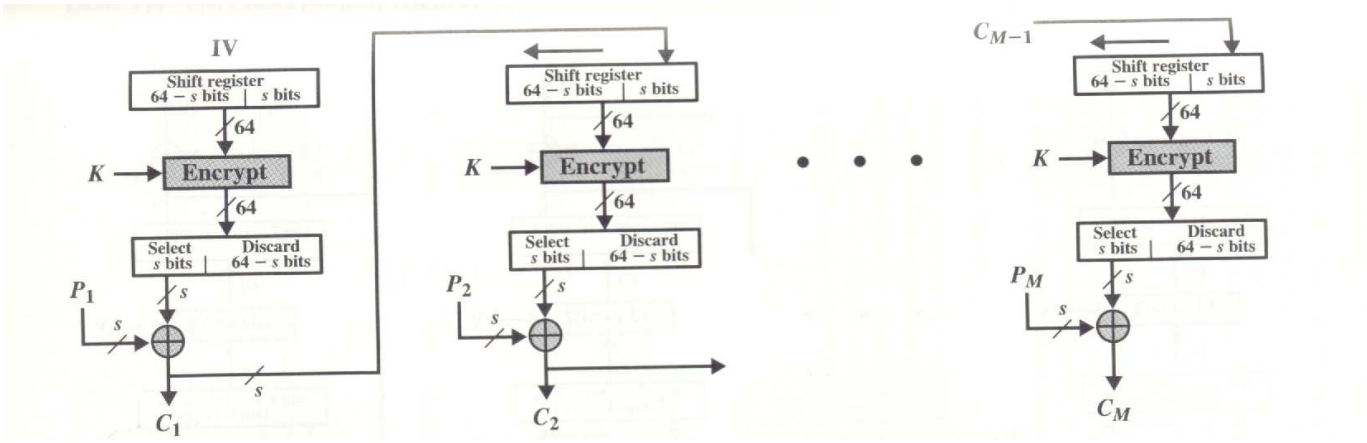


Figura 1: Cifrado para el modo de operacion CFB.

17. Respecto al DES explicar detalladamente sus fundamentos: confusión y difusión, producto de criptosistemas y cifrado Feistel. Escribe en un diagrama cuál es la estructura de cifrado y la de descifrado.

18. Respecto a DES responde a estas preguntas razonadamente:

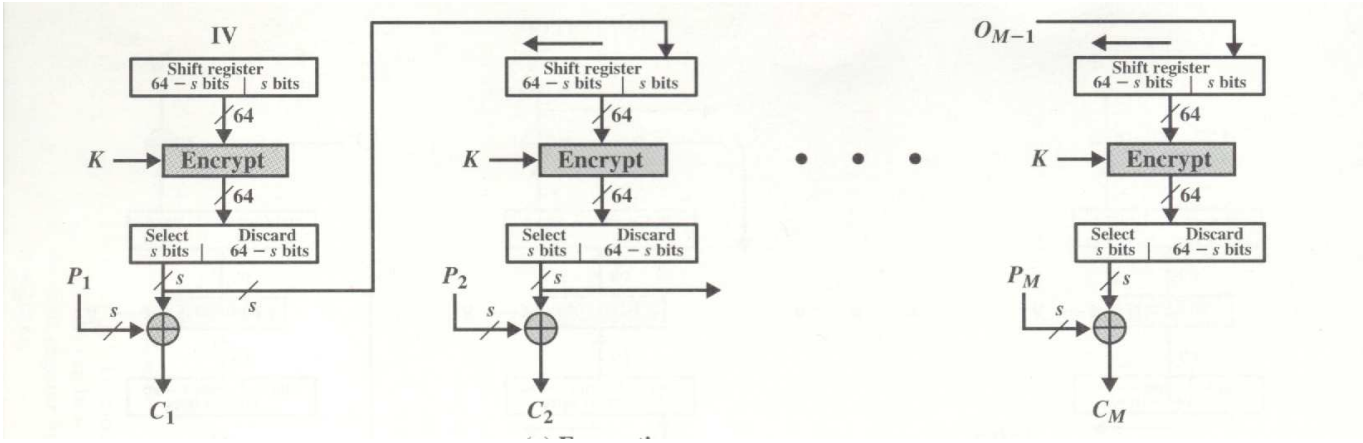


Figura 2: Cifrado para el modo de operacion OFB.

19. Explica en que consiste el ataque en el medio para este sistema criptográfico.

20. Calcula la distancia de unicidad para el DES doble y el DES triple razonando los resultados que se obtienen.

21. Calcula el inverso de x^2 en el $GF(2^3)$, con $m(x) = x^3 + x + 1$.

22. Calcula el inverso de $x^7 + 1$ en el $GF(2^8)$ del AES.

23. Efectúa el producto de polinomios $(x^6 + x^4 + x^2 + x + 1)(x^7 + x + 1)$, reduciendo posteriormente por $m(x) = x^8 + x^4 + x^3 + x + 1$.

24. Demuestra que $x^8 \; mod \; m(x) = m(x) - x^8$, con $m(x) = x^8 + x^4 + x^3 + x + 1$.

25. Calcula '23´ • '81' usando la función xtime del AES de tal manera que se usen el menor número de operaciones posibles.

26. Da el pseudocódigo de un algoritmo eficiente para la implementación de la función xtime.

27. Da el pseudocódigo de un algoritmo eficiente para la implementación del producto de polinomios sobre $GF(2^8)$ del AES, basado en la función xtime. Compara este algoritmo en rendimiento con otro que implemente xtime en una tabla de 256 valores. Compara estos dos algoritmos con otro que utilice tablas logarítmicas y antilogarítmicas para multiplicar

los polinomios sobre $GF(2^8)$ del AES (ver "A Specification for The AES Algorithm" Dr. Briam Gladman, v3.6, 15^{th} April 2003, pp 4–5).

28. Demostrar que dividir x^j por $x^4 + 1$ es equivalente a $x^{j \, mod \, 4}$, en el problema AES.

29. Demostrar que la transformación afín en la función `InvByteSub(State)` es realmente la transformación inversa de la función afín que se emplea en `ByteSub(State)`.

30. Demostrar que las funciones `ByteSub(State)` y `InvByteSub(State)` son equivalentes a las cajas S y S^{-1} del AES.

31. Demostrar que los producto matricial de los inversos multiplicativos que se utilizan en las funciones `ByteSub(State)` y `InvByteSub(State)` son equivalentes a las transformaciones:

$$b_i = a'_i \oplus a_{(i+4)mod8} \oplus a_{(i+5)mod8} \oplus a_{(i+6)mod8} \oplus a_{(i+7)mod8} \oplus c_i$$

para la función`ByteSub(State)`, y

$$a'_i = b_{(i+2)mod8} \oplus b_{(i+5)mod8} \oplus b_{(i+7)mod8} \oplus d_i$$

para para la función `InvByteSub(State)`.

32. Demostrar que las matrices de multiplicación de las funciones `MixColumn(State)` y `InvMixColumn(State)` son una es la inversa de la otra.

33. Demuestra que el producto del polinomio $03x^3 + 01x^2 + 01x + 02$ por la columna del estado del AES en la transformación `MixColumn` se puede expresar como el producto de matrices explicado en la teoría.

34. Demuestra que las funciones `ByteSub` y `ShiftRow` del AES son conmutativas.

35. Da en pseudocódigo cómo tiene que ser el algoritmo de inversión de la llave en la transformada inversa del AES equivalente.

36. Estudia como se puede implementar de una manera óptima el AES para un procesador de 8 bits. Consulta la bibliografía de la asignatura.

37. Explica qué relación existe entre los polinomios de grado 3 con coeficientes en $GF(2^8)$ y el AES. Nombra cuáles son la funciones típicas de una ronda de cifrado de AES indicando qué tipo de operaciones básicas se realiza en cada una de ellas.

38. Estudiar el proceso de avalancha en el AES para el mensaje y la clave en función de las rondas.

39. Dado el byte (10000001) ¿cuál es su transformación a través de la función de sustitución de bytes del algoritmo de encriptación AES? Recuerda que el polinomio irreducible en $GF(2^8)$ es $m(x) = x^8+x^4+x^3+x+1$, y que la transformación afín viene determinada por:

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} a'_0 \\ a'_1 \\ a'_2 \\ a'_3 \\ a'_4 \\ a'_5 \\ a'_6 \\ a'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Razona todos los resultados.

40. Dado el byte (00001001) ¿cuál es su transformación a través de la función de sustitución de bytes del algoritmo de encriptación AES? Recuerda que el polinomio irreducible en $GF(2^8)$ es $m(x) = x^8+x^4+x^3+x+1$, y que la transformación afín viene determinada por:

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \\ a_4 \\ a_5 \\ a_6 \\ a_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}$$

Razona todos los resultados.

41. Dado el byte $6F$, ¿cuál es su transformación a través de la función de sustitución de bytes inversa del algoritmo de encriptación AES? Recuerda que el polinomio irreducible en $GF(2^8)$ es $m(x) = x^8 + x^4 + x^3 + x + 1$, y que la transformación afín inversa viene determinada por:

$$\begin{pmatrix} a'_0 \\ a'_1 \\ a'_2 \\ a'_3 \\ a'_4 \\ a'_5 \\ 'a_6 \\ a'_7 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ a_b \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Razona todos los resultados.

42. Deduce la expresión general para optimizar el producto por x por un polinomio $b(x)$ (i.e. $xtime(b(x))$ en el AES), donde este polinomio pertenece al espacio de $GF(2^8)/m(x)$ con $m(x) = x^8 + x^4 + x^3 + x + 1$. Aplica esta función de $xtime()$ del AES a la operación '57´ • '13'. Escribe un pseudocódigo para multiplicar 2 polinomios en $GF(2^8)/m(x)$ a través de la función $xtime()$. Razona todos los resultados.