Criptografía y Seguridad, Tarea 2

Fecha de Entrega: Lunes 15 de abril de 2013

1. Una propiedad importante en la seguridad de DES es que las cajas-S no son lineales. Muestra que $S_1(x_1) \oplus S_1(x_2) \neq S_1(x_1 \oplus x_2)$, para:
   (a) $x_1 = 000000, x_2 = 000001$
   (b) $x_1 = 111111, x_2 = 100000$
   (c) $x_1 = 101010, x_2 = 010101$
2. ¿Cuál es la salida en la primera ronda del algoritmo DES cuando el texto claro y la llave son todos 1?
3. Usando en DES una palabra de entrada que tiene un 1 en el bit 57 y en todos los demás 0, y una llave de puros ceros:
   (a) ¿Cuantas cajas-S tienen una entrada diferente comparado con el caso en que todos los bits de la palabra de entrada son cero?
   (b) ¿Cuál es la salida después de la primera ronda?
   (c) ¿Cuantos bits de salida cambiaron después de la primera ronda, respecto a el caso en que todos los bits de la palabra de entrada son cero?
4. Sean $p = 41$ y $p = 17$ los dos primos dados como parámetros de RSA.
   (a) ¿Cuál de los parámetros $e_1 = 32, e_2 = 49$ es un exponente valido para RSA?
   (b) Calcula la llave privada correspondiente $k_{pr} = (p, q, d)$
5. Cifra y descifra usando el algoritmo RSA con los siguientes parámetros:
   (a) $p = 3, q = 11, d = 7, x = 5$
   (b) $p = 5, q = 11, e = 3, x = 9$
6. Dado un esquema de firma digital con RSA y llave publica ($n = 9797, e = 131$), ¿Cuáles de las siguientes firmas es valida?
   (a) $(x = 123, sig(x) = 6292)$
   (b) $(x = 4333, sig(x) = 4768)$
   (c) $(x = 4333, sig(x) = 1424)$