Parcial 1

7 de septiembre de 2020

Indicaciones generales

- Este es un examen **individual** con una duración de **110 minutos: de 9:00 a 10:50**.
- No se permite la comunicación con otra persona ni consultas en inter o apuntes de clase.
- No se permite el uso de libros o apuntes, cualquier medio electrónico distinto a una calculadora. Los celulares deben estar apagados durante todo el examen.
- Las respuestas deben estar totalmente justificadas.
- Se permitirá hacer preguntas sobre el enunciado al profesor, en voz alta, hasta las 9:20 únicamente.
- Cualquier incumplimiento de lo anterior conlleva a la anulación del examen.
- Al entregar este parcial usted está jurando bajo su honor que no está comentiendo ningun tipo de actividad que incumpla lo anterior ni el reglamento estudiantil.
- Durante las 10h50 y las 11h00 usted deberá subir las fotos de su parcial a e-aulas, tendrá tiempo hasta las 11:20 para subir el pdf conlas fotos enumerdadas y marcadas de buena calidad.

Ejercicio 1 [1 punto.] Utilizando el Teorema del Residuo Chino, encuentre el $0 \leq x \leq 91$ tal que

$$\begin{cases} x \equiv 3 \bmod 7 \\ x \equiv 5 \bmod 13 \end{cases}$$

Ejercicio 2 [1 punto.]

Asuma que sabemos que Alice y Bob se comunican utilizando el Cifrado *Affine* y que se interceptaron los siguientes pares textos plano, textos cifrado:

$$(m_1, c_1) = (2, 12) \text{ y } (m_2, c_2) = (5, 3).$$

Encuentre la clave secreta que usaron Alice y Bob para cifrar. Justifique su respuesta.

Ejercicio 3 [1 punto.]
A continuación, asumamos que $\overline{x}$ denota la cadena de bits que se obtienen al intercambiar en un acadena de bits x los $0's$ por un 1 y los $1's$ por un 0.

Considere las claves k y $\overline{k}$ del criptosistema DES y los textos de 64-bits x y $\overline{x}$. Asuma que en el momento de generar las claves de cada ronda en el DES si se usa $\overline{k}$ en vez de k vamos a obterner que en la fila i, la subclave es $\overline{k_i}$, donde k_i es la subclave de k en la ronda i.

Sea $c = e_k(m)$ y $c' = e_{\overline{k}}(\overline{m})$. Muestre que $c' = \overline{c}$.

Ejercicio 4 [1 punto.]

Asuma que se está cifrando con criptosistema simetrico de bloques (de $n-$bits) y que se están transmitiendo los c_i.

1. Asuma que se está usando el modo ECB y discuta que pasa si:
   a) Uno de los c_i se daña en la transmisión.
   b) Uno de los c_i se pierde en la transmisión.
2. Asuma que se está usando el modo CBC y discuta que pasa si:
   a) Uno de los c_i se daña en la transmisión.
   b) Uno de los c_i se pierde en la transmisión.
3. Asuma que se está usando el modo OFB y discuta que pasa si:
   a) Uno de los c_i se daña en la transmisión.
   b) Uno de los c_i se pierde en la transmisión.
4. Asuma que se está usando el modo *Counter* y discuta que pasa si:
   a) Uno de los c_i se daña en la transmisión.
   b) Uno de los c_i se pierde en la transmisión.

Ejercicio 5 [1 punto.]

Asuma que se está cifrando con el cifrado RC4, con $w = 3$, $s = 3$, la clave secreta es $k = (2, 6, 4)$ y que la tabla para cifrar S está dada por:

a	0	1	2	3	4	5	6	7
$S(a)$	1	7	4	3	5	2	6	0

1. Encuentre z_1, z_2, z_3 y z_4.
2. Cifre los mensajes $m_1 = 101$ y $m_2 = 110$.
3. Descifre $c_3 = 111$ y $c_4 = 010$.