Parcial 32

11 de noviembre 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 [1,1 puntos.]
Considere la variantes del CBC-MAC: Asuma que el valor inicial es elegído aleatoriamente y enviado con el mensaje y con el MAC. Muestre por qué esta propuesta no es segura y existe una falsificación trivial.

Ejercicio 2 [1,2 puntos.]

Considere un $(3, 5)$-*threshold secret sharing system* de Shamir, con $p = 7$. Tenemos 5 *shareholders* con las siguientes parejas (x_i, y_i) : $(1, 6), (2, 5), (3, 6), (4, 2)$ y $(5, 0)$.

Encuentre la clave secreta k.

Ejercicio 3 [1,5 puntos.]

1. Explique por qué es mala idea usar $MAC_K(X) = H(K|X)$, con H una función de Hash iterada, K secreta y $a|b$ quiere decir que se concatena b a la cadena a.

2. Diga 2 diferencias entre la autenticación usando MAC y usando firmas digitales.

Ejercicio 4 [1,2 puntos.]

1. Explique la firma del RSA

2. Explique la firma de El-Gamal