# Parcial 2

14 de octubre 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.]
Considere el criptosistema RSA con un modulo $n$ grande, de 1000 bits. Imagine un escenario en el que ciframos 2 bytes a las vez. Sea $m_1$ y $m_2$ dos bytes, entonces $m = (m_1, m_2)$ a la vez:

$$c = (m_1.2^8 + m_2)^e \mod n,$$

donde $(e, n)$ es la clave secreta del RSA. Muestre como atacar el sistema.

**Ejercicio 2** [1 punto.]

Alice le quiere enviar un correo a Bob usando el criptosistema de El-Gamal. Alice aprendió a no repetir el valor aleatorio $k$. Alice decide entonces escoger un $k$ aleatorio para cifrar el mensaje $m$, luego utiliza $k+1$ para cifrar $m_1$, luego $k+2$ para cifrar $m_2$, y así susecivamente. Muestre que eso no es una buena idea. Justifique su respuesta.

**Ejercicio 3** [1 punto.]
Considere la función de Hash basada en modulo aritmético modulo un número primo. Sea $p$ un primo fijo y público. Definimos la función de Hash iterada, con la construcción Merkle-Damgard, dónde la función de compresión es

$$h_i = h_{i-1} x_i \mod p,$$

donde $x_1, \ldots, x_t$ son los mensages en bloque (ya incluídos los bits del padding) y donde $h_0$ es un valor inicial público. Adicionalmente asumimos que $h_0 \neq 0 \mod p$ y que $x_i \neq 0 \mod p$ para todo $i$. Definamos el hash de $x = (x_1, \ldots, x_t)$ como $H(x) = h_t$.

1. Encuentre una colision para esta función de Hash.
2. Dado un mensaje de 3 bloques $y = (y_1, y_2, y_3)$, encuentre una segunda preimagen de $H(y)$.

**Ejercicio 4** [1 punto.]

En la misma época en la que el RSA fué inventado, Pohlig-Hellman propusieron el siguiente sitema: sea $p$ un número primo, escoja $a$ aleatoriamente en $\mathbb{Z}_{p-1}^*$ y calcule $b = a^{-1} \mod (p-1)$. La clave secreta es $a$ y la clave pública $(b, p)$. El cifrado está definido por:

$$e_k(m) = m^b \mod p$$

y el decifrado esta definido por

$$d_k(c) = c^a \mod p.$$

1. Muestre que si $c = m^b \mod p$, entonces $c^a = m \mod p$.
2. Muestre por qué NO es una buena idea usar este sistema como un criptosistema a clave pública.

(Nota: Pohlig-Hellman, no propusieron este sitema como un criptosistema a clave pública.)

**Ejercicio 5** [0.5 puntos.]

Considere la siguiente regla de padding, donde $(N - n)$ es el largo del bloque del mensaje.

- Sea $x \in \{0, 1\}^v$ la cadena de $v$ bits a la que se le quiere sacar el hash.
- Agregue un 1 al final de $x$.
- Sea $s$ el menor entero positívo tal que $v + 1 + s$ sea un multiplo de $N - n$.
- Agregue $s$ zeros al final de $x|1$.

Sean $x$ y $y$ dos cadenas de bits y sea $pad(x)$ y $pad(y)$ los padding de las dos cadenas. Decimos que la regla de padding es libre de colisiones si $x \neq y$ implica que $pad(x) \neq pad(y)$. Demuestre que el padding explicado anteriormente es libre de colisiones o de un contra ejemplo.