DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN
ESCUELA DE INGENIERÍA
PONTIFICIA UNIVERSIDAD CATÓLICA DE CHILE

IIC3253 - Criptografía y Seguridad Computacional (I/2023)

Ayudantía 4

Ayudantes: Susana Figueroa (sfigueroa3@uc.cl)

Pregunta 1: Operaciones con polinomios

(a) Calcule las siguientes divisiones de polinomios:
1. $x^3 + x^2 + x + 1 \ / \ x + 9$
2. $7x^3 - 1 \ / \ x + 2$
3. $5x^4 + x^2 - 8x + 2 \ / \ x - 4$

(b) Calcule las raíces de los siguientes polinomios:
1. $x^2 - 1$ en $mod\ 5$
2. $x^2 - 3x + 2$ en $mod\ 3$
3. $x^3 + 3x^2 + 5x + 3$ en $mod\ 6$

(c) Calcule los siguientes módulos, en módulo 2:
1. $x^{12} \ mod \ x^8 + x^4 + x^3 + x + 1$
2. $x^3 + 7x^2 + 9 \ mod \ x^2 + 3$
3. $5x^5 - 4x^3 + 2x \ mod \ x^4 + 2x$

Pregunta 2: Intercambio de llaves

Todos los algoritmos que han visto en clases hasta ahora se ha asumido que los participantes se han "juntado en el parque" previamente para compartir la llave que van a utilizar para encriptar sus mensajes. Claramente en la práctica esto no ocurre. El objetivo de este ejercicio es diseñar un algoritmo que permita compartir un "secreto" entre dos participantes y que no pueda ser descubierto **fácilmente** por un tercero.

Alice quiere tener una comunicación segura y privada con Bob, para poder lograr esto se tienen que poner de acuerdo en una llave simétrica para encriptar sus mensajes. Debido a sus horarios, no pueden juntarse ningún día para acordar la llave, por lo que tu deberás idear un algoritmo criptográfico para que puedan decidir en una llave de forma remota. Este algoritmo tiene que cumplir con:

- Alice es la encargada de diseñar la llave.
- Para Bob debe ser relativamente fácil descubrir cual es la llave.
- Para cualquier persona externa le debe ser más difícil que a Bob encontrar la llave acordada.
- Las personas externas solo pueden escuchar el canal de comunicación entre Alice y Bob, no pueden mandar mensajes ni manipularlos.
- Todos conocen el método de encriptación.
- Las funciones de encriptación y decriptación son $\mathcal{O}(1)$.