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. $5x^4 + x^2 - 8x + 2 \ / \ x - 4$

Solución:

1. $x^3 + x^2 + x + 1 \ / \ x + 9$

   Partimos preguntando, cuantas veces cabe el $x + 9$ en $x^3 + x^2 + x + 1$. Cabe x^2 veces.

$$\begin{array}{rl} & x^3 + x^2 + x + 1 \ / \ x + 9 = x^2 \\ - & \underline{x^3 + 9x^2} \\ & 0 - 8x^2 + x + 1 \end{array}$$

   Ahora, cuantas veces cabe el $x + 9$ en $-8x^2 + x + 1$. Cabe $-8x$ veces.

$$\begin{array}{rl} & x^3 + x^2 + x + 1 \ / \ x + 9 = x^2 - 8x \\ - & \underline{x^3 + 9x^2} \\ & 0 - 8x^2 + x + 1 \\ - & \underline{\quad - 8x^2 - 72x} \\ & 0 + 73x + 1 \end{array}$$

Ahora, cuantas veces cabe el $x+9$ en $73x+1$. Cabe 73 veces.

$$
\begin{array}{rl}
 & x^3+x^2+x+1 \ / \ x+9 = x^2-8x+73 \\
- & \underline{x^3+9x^2} \\
 & 0-8x^2+x+1 \\
- & \underline{\quad -8x^2-72x} \\
 & 0+73x+1 \\
- & \underline{\quad 73x+657} \\
 & -656
\end{array}
$$

Entonces, el resultado de la división es

$$x^3+x^2+x+1 \ / \ x+9 \ = \ x^2-8x+73-\frac{656}{(x+9)}$$

2. $7x^3-1 \ / \ x+2$

$$
\begin{array}{rl}
 & 7x^3-1 \ / \ x+2 = 7x^2-14x+28 \\
- & \underline{7x^3+14x^2} \\
 & 0-14x^2-1 \\
- & \underline{\quad -14x^2-28x} \\
 & 0+28x-1 \\
- & \underline{\quad 28x+56} \\
 & -57
\end{array}
$$

Entonces, el resultado de la división es

$$7x^3-1 \ / \ x+2 \ = \ 7x^2-14x+28-\frac{57}{(x+2)}$$

3. $5x^4 + x^2 - 8x + 2 \ / \ x - 4$

$$
\begin{array}{rl}
 & 5x^4 + x^2 - 8x + 2 \ / \ x - 4 = 5x^3 + 20x^2 + 81x + 316 \\
- & \underline{5x^4 - 20x^3} \\
 & 0 + 20x^3 + x^2 - 8x + 2 \\
- & \underline{\ \ 20x^3 - 80x^2} \\
 & \ \ 0 + 81x^2 - 8x + 2 \\
- & \underline{\ \ \ 81x^2 - 324x} \\
 & \ \ \ 0 + 316x + 2 \\
- & \underline{\ \ \ \ 316x - 1264} \\
 & \ \ \ \ \ \ 1266
\end{array}
$$

Entonces, el resultado de la división es

$$5x^4 + x^2 - 8x + 2 \ / \ x - 4 \ = \ 5x^3 + 20x^2 + 81x + 316 - \frac{1266}{(x-4)}$$

(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 $mod\ 6$

Solución:

1. $x^2 - 1$ en $mod\ 5$

   Como estamos buscando las raíces de $f(x) = x^2 - 1$ en módulo 5, necesitamos que la raíz evaluada en el polinomio módulo 5 sea 0.

   $$f(r)\ mod\ 5 = 0$$

   Partimos factorizando la expresión,

   $$x^2 - 1 = (x-1)(x+1)$$

Entonces, nuestras raíces serian $x_1 = 1$ y $x_2 = -1$. Pero tenemos un problema, $x_2 \notin \{0, ..., 4\}$, falta calcularle el módulo.

$$x_2 \ mod\ 5 = -1 \ mod\ 5 = 4$$

Entonces, nuestras raíces son $x_1 = 1$ y $x_2 = 4$.

$$x^2 - 1 \ \ mod\ 5 \ = \ (x-1)(x-4) \ \ mod\ 5$$

2. $x^2 + 2x - 3$ en $mod\ 3$

   Factorizamos,

$$x^2 + 2x - 3 = (x-1)(x+3)$$

   Tenemos que nuestras raíces son $x_1 = 1$ y $x_2 = -3$. Nuevamente $x_2 \notin \{0, ..., 4\}$, le calculamos el módulo.

$$x_2 \ mod\ 3 = -3 \ mod\ 3 = 0$$

   Entonces, nuestras raíces son $x_1 = 1$ y $x_2 = 0$.

$$x^2 + 2x - 3 \ \ mod\ 3 \ = \ (x-1)x \ \ mod\ 3$$

3. $x^3 + 3x^2 + 5x + 3$ en $mod\ 6$

   Ahora vamos a intentar otro método, partimos buscando una raíz. Al ojimetro podemos ver que $x_1 = 1$ es una raíz (en módulo 6).

$$\begin{aligned} f(1) \ \ mod\ 6 &= (1)^3 + 3(1)^2 + 5(1) + 3 \ \ mod\ 6 \\ &= 1 + 3 + 5 + 3 \ \ mod\ 6 \\ &= 12 \ \ mod\ 6 = 0 \end{aligned}$$

   Aplicando lo que vimos en la sección anterior, dividimos $x^3 + 3x^2 + 5x + 3$ por $x - 1$. Como sabemos que $x - 1$ es una raíz, la división no debería tener resto (en módulo 6).

$$
\begin{array}{rl}
 & x^3+3x^2+5x+3 \;\;/\;\; x-1 = x^2+4x+9 \\
- & x^3-x^2 \\
\hline
 & 0+4x^2+5x+3 \\
- & \quad 4x^2-4x \\
\hline
 & \quad 0+9x+3 \\
- & \quad\;\; 9x-9 \\
\hline
 & \quad\;\; 0+12
\end{array}
$$

Podemos olvidarnos del resto, porque como estamos en módulo 6, $12 \; mod \; 6 = 0$. También,

$$x^2+4x+9 \;\; mod \; 6 = x^2+4x+3 \;\; mod \; 6$$

Si factorizamos x^2+4x+3.

$$x^2+4x+3 = (x+3)(x+1)$$

Pero $x_2 = -3 \notin \{0,...,5\}$ y $x_3 = -1 \notin \{0,...,5\}$. Debemos calcular sus módulos.

$$-3 \;\; mod \; 6 = 3$$
$$-1 \;\; mod \; 6 = 5$$

Entonces, nuestras raíces son $x_1 = 1$, $x_2 = 3$ y $x_3 = 5$.

$$x^3+3x^2+5x+3 \;\; mod \; 6 \;\; = \;\; (x-1)(x-3)(x-5) \;\; mod \; 6$$

(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. $5x^5 - 4x^3 + 2x \ \ mod \ \ x^4 + 2x$

Solución:

1. $x^{12} \ \ mod \ \ x^8 + x^4 + x^3 + x + 1$

   Partimos preguntándonos, cuantas veces cabe $x^8 + x^4 + x^3 + x + 1$ en x^{12}. Cabe x^4 veces, calculamos la división para obtener el resto.

$$\begin{array}{rl} & x^{12} \ / \ x^8 + x^4 + x^3 + x + 1 = x^4 \\ - & x^{12} + x^8 + x^7 + x^5 + x^4 \\ \hline & 0 - x^8 - x^7 - x^5 - x^4 \end{array}$$

   Como estamos en módulo 2,

$$\begin{aligned} \left(x^{12} \ \ mod \ \ x^8 + x^4 + x^3 + x + 1\right) \ \ mod \ \ 2 &= \left(-x^8 - x^7 - x^5 - x^4\right) \ \ mod \ \ 2 \\ &= \left(x^8 + x^7 + x^5 + x^4\right) \ \ mod \ \ 2 \end{aligned}$$

2. $x^3 + 7x^2 + 9 \ \ mod \ \ x^2 + 3$

   Para tener el resto debemos dividir $x^3 + 7x^2 + 9$ por $x^2 + 3$.

$$\begin{array}{rl} & x^3 + 7x^2 + 9 \ / \ x^2 + 3 = x + 7 \\ - & x^3 + 3x \\ \hline & 0 + 7x^2 - 3x + 9 \\ - & 7x^2 + 21 \\ \hline & 0 - 3x - 12 \end{array}$$

Como estamos en módulo 2,

$$\begin{aligned}\Big(x^3+7x^2+9 \ \ mod \ \ x^2+3\Big) \ \ mod \ \ 2 &= \Big(-3x-12\Big) \ \ mod \ \ 2\\ &= \Big(x\Big) \ \ mod \ \ 2\end{aligned}$$

3. $5x^5-4x^3+2x \ \ mod \ \ x^4+2x$

   Calculemos el resto.

$$\begin{array}{rl} & 5x^5-4x^3+2x \ \ / \ \ x^4+2=5x \\ - & \underline{5x^5+10x} \\ & 0+-4x^3-8x \end{array}$$

Como estamos en módulo 2,

$$\begin{aligned}\Big(5x^5-4x^3+2x \ \ mod \ \ x^4+2\Big) \ \ mod \ \ 2 &= \Big(-4x^3-8x\Big) \ \ mod \ \ 2\\ &= \big(0\big) \ \ mod \ \ 2\end{aligned}$$

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 $\mathcal{O}(1)$.

Solución:

Este problema lo resolvió Ralph Merkle en el año 1978, no se utiliza en la práctica pero es interesante :)

La idea de Merkle es crear varios *puzzles* que estén diseñados para ser rotos. Bob elige uno de estos *puzzles*, lo resuelve y le informa a Alice cual resolvió. Eve (persona externa), no sabe cual *puzzle* eligió Bob, por lo que debe resolverlos todos para poder espiar la conversación.

Vamos a hacer una versión alternativa a la propuesta en su *paper*. Si quieres revisar cual es el método original puedes leer "Secure Communications Over Insecure Channels".

Primero se debe partir eligiendo una función de encriptación fuerte y el n (cantidad de *puzzles*) a usar. Ambos deben ser comunicados a través del canal, es decir que todos conocen estos parámetros. Después debemos crear nuestros *puzzles*, cada uno de ellos deben contener al menos dos cosas: una llave y un identificador.

Entonces, Alice va a crear n *puzzles*. Cada uno va a ser de la forma:

$$p_i = Enc_{d_i}\big(d_i \mid\mid k_i \# ID_i\big)$$

Siendo d_i con $i \in \{1, \ldots, n\}$, una llave (del puzzle) elegida aleatoriamente y $d_i \in \{0,1\}^{log(n)}$. También k_i y ID_i deben elegidos de manera aleatoria.

Alice envía estos n mensajes a través del canal de comunicación a Bob. Eve también recibe todos estos mensajes.

Ahora es el turno de Bob. El debe elegir uno de estos n *puzzles* y resolverlo "a la mala". Debe probar todas las llaves $x_j \in \{0,1\}^{log(n)}$ hasta encontrar una tal que:

$$Dec_{x_j}(p_i) = x_j \mid\mid y$$

Si encontramos una llave x_j tal que al decriptar p_i con x_j, el mensaje empieza con la misma llave, logramos resolver el *puzzle*. Como lo logramos decifrar, sabemos que el mensaje que sigue después de x_j corresponde a la llave que queremos utilizar después en la comunicación y el ID del *puzzle*.

Este ID es importante porque de alguna forma le queremos comunicar a Alice que logramos resolver el *puzzle* i. Y como este ID_i fue generado de manera aleatoria por Alice, podemos mandárselo de vuelta a través del canal, sin cifrar. Eve puede ver este mensaje, pero no le aporta información, igual deberá tratar de resolver todos los *puzzles* hasta encontrar uno que al resolverlo le de el ID que Bob le mando a Alice.

Entonces, Bob le manda a Alice el ID_i, Alice revisa a cual *puzzle* esta asociado ese ID. Ahora ambos conocen la llave k_i y la pueden usar para comunicarse de manera segura.

Cúal es la complejidad de todo esto??

- Alice: La complejidad de crear los n *puzzles* es $\mathcal{O}(n)$.
- Bob: La complejidad de decriptar un *puzzle* es de $\mathcal{O}(n)$, dado que tiene que probar $2^{log(n)} = n$ llaves.
- Eve: Como debe resolver todos los *puzzles*, la complejidad es $\mathcal{O}(n^2)$.