SOLUCIONES PRUEBA DE MATEMÁTICA DISCRETA

1. (a) Sabiendo que la clave pública es $n = 10553$ ($n = 173 \cdot 61$) y $e = 191$, calcular la clave privada y decir como se encripta y descifra un mensaje con el sistema RSA.

(b) Calcular A y B sabiendo que el número $119A2692B63$ es múltiplo de 9 y de 11.

Solución:

(a) Cálculo de la clave privada d: $\phi(n) = \phi(10553) = (173 - 1) \cdot (61 - 1) = 172 \cdot 60 = 10320$.

d es el inverso modular de $e = 191$ módulo $\phi(n) = 10320$.

$\gcd(10320, 191) = 1$, ya que

$$\begin{array}{r|l} 10320 & 191 \\ \hline 6 & 54 \end{array} \qquad \begin{array}{r|l} 191 & 6 \\ \hline 5 & 31 \end{array} \qquad \begin{array}{r|l} 6 & 5 \\ \hline 1 & 1 \end{array}$$

$6 = 10320 - 54 \cdot 191, \qquad 5 = 191 - 31 \cdot 6, \qquad 1 = 6 - 1 \cdot 5.$

Así:

$$1 = 6 - 5 = 6 - (191 - 31 \cdot 6) = 32 \cdot 6 - 191 = 32 \cdot (10320 - 54 \cdot 191) - 191$$
$$= 32 \cdot 10320 - 1728 \cdot 191 - 191 = 32 \cdot 10320 - 1729 \cdot 191$$

Por lo tanto, el inverso modular de 191 módulo 10320 es -1729, pero

$$-1729 \equiv 8591 \bmod 10320.$$

Para encriptar un mensaje m;

$$m \longrightarrow m^{191} \bmod 10533.$$

Para descifrar el mensaje recibido x;

$$x \longrightarrow x^{8591} \bmod 10533.$$

(b)

$$119A2692B63 \equiv A + B + 3 \bmod 9$$

Por lo tanto $119A2692B63$ es divisible por 9 si, y solo si,

$$A + B + 3 \equiv 0 \bmod 9 \Longleftrightarrow A + B \equiv 6 \bmod 9$$

Por otro lado,

$$119A2692B63 \equiv -A + B - 2 \bmod 11$$

Por lo tanto $119A2692B63$ es divisible por 11 si, y solo si,

$$-A + B - 2 \equiv 0 \bmod 11 \Longleftrightarrow B - A \equiv 2 \bmod 11$$

Las posibles soluciones de $A + B \equiv 6 \bmod 9$ son:

A	B
0	6
1	5
2	4
3	3
4	2
5	1
6	0 o 9
7	8
8	7
9	6

La única solución que verifica $B - A \equiv 2 \bmod 11$ es $A = 2$ y $B = 4$. Por lo tanto el número es: 11922692463.

2. (a) Sabiendo que la clave pública es $n = 9853$ ($n = 167 \cdot 59$) y $e = 187$, calcular la clave privada y decir como se encripta y descifra un mensaje con el sistema RSA.

(b) Calcular A y B sabiendo que el número $39A4230B21$ es múltiplo de 3 y de 11.

Solución:

(a) Cálculo de la clave privada d: $\phi(n) = \phi(9853) = (167-1)\cdot(59-1) = 166\cdot 58 = 9628$. d es el inverso modular de $e = 187$ módulo $\phi(n) = 9628$.
$\gcd(9628, 187) = 1$, ya que

$$\begin{array}{l|l} 9628 & 187 \\ \cline{2-2} 91 & 51 \end{array} \qquad \begin{array}{l|l} 187 & 91 \\ \cline{2-2} 5 & 2 \end{array} \qquad \begin{array}{l|l} 91 & 5 \\ \cline{2-2} 1 & 18 \end{array}$$

$91 = 9628 - 51 \cdot 187, \qquad 5 = 187 - 2 \cdot 91, \qquad 1 = 91 - 18 \cdot 5.$

Así:

$$\begin{aligned} 1 &= 91 - 18 \cdot 5 = 91 - 18 \cdot (187 - 2 \cdot 91) = 37 \cdot 91 - 18 \cdot 187 \\ &= 37 \cdot (9628 - 51 \cdot 187) - 18 \cdot 187 = 37 \cdot 9628 - 1905 \cdot 187 \end{aligned}$$

Por lo tanto, el inverso modular de 187 módulo 9628 es -1905, pero

$$-1905 \equiv 7723 \bmod 9628.$$

Para encriptar un mensaje m;

$$m \longrightarrow m^{187} \bmod 9853.$$

Para descifrar el mensaje recibido x;

$$x \longrightarrow x^{7723} \bmod 9853.$$

(b)

$$39A4230B21 \equiv A + B \bmod 3$$

Por lo tanto $39A4230B21$ es divisible por 3 si, y solo si,

$$A + B \equiv 0 \bmod 3$$

Por otro lado,

$$39A4230B21 \equiv -A + B - 1 \bmod 11$$

Por lo tanto $39A4230B21$ es divisible por 11 si, y solo si,

$$-A + B - 1 \equiv 0 \bmod 11 \Longleftrightarrow B - A \equiv 1 \bmod 11$$

Las posibles soluciones de $A + B \equiv 0 \bmod 3$ son:

A	B
0	0 o 3 o 6 o 9
1	2 o 5 o 8
2	1 o 4 o 7
3	0 o 3 o 6 o 9
4	2 o 5 o 8
5	1 o 4 o 7
6	0 o 3 o 6 o 9
7	2 o 5 o 8
8	1 o 4 o 7
9	0 o 3 o 6 o 9

Las posibles soluciones que verifica $B - A \equiv 1 \bmod 11$ son:

- $A = 1$ y $B = 2$. Por lo tanto el número es: 3914230221.
- $A = 4$ y $B = 5$. Por lo tanto el número es: 3944230521.
- $A = 7$ y $B = 8$. Por lo tanto el número es: 3974230821.

Por lo tanto los números posibles son:
3914230221, 3944230521, 3974230821.