Evaluación 3: Parte 1

Carrillo García Aldo

Hernández Flores Luis Ángel

Macedo Madrigal Rodrigo

Polo Monroy Ricardo

Vázquez Andrés Mónica

2020 Enero

1. Ejercicio 1

¿ Cuál es la clave común que deben usar dos individuos que han escogido como claves los números $k_1 = 21$ y $k_2 = 83$, si el módulo es $p = 719$ y $a = 5$?

Solución:

Usando el algoritmo de Diffie-Helman podemos obtener la llave que se utiliza en común, ya que

$$k = a^{k_1 k_2} \bmod \text{p}$$

De esta forma tenemos

$$k = 5^{21*83} \bmod 719$$

$$k = 5^{1743} \bmod 719$$

$$k = 406$$

Así, la llave en común de ambos individuos es: $k = 406$

2. Ejercicio 2

Si $p = 6833$, $a = 15$ y tres individuos escogen como claves $k_1 = 3$, $k_2 = 25$ y $k_3 = 45$, ¿qué número pueden usar como clave común?

Solución:

Ya conocemos como sacar la llave cuando tenemos solo dos individuos y ahora necesitamos ver que hacer cuando se aumenta un individuo. Sabiendo que $y_n = a^{k_n}$ mód p y que con dos individuos $k = y_1^{k_2}$ mód p y $k = y_2^{k_1}$ llegamos a que

$$k = a^{k_1 k_2} \text{ mód p}$$

Teniendo al tercer intregante el valor tendría que pasar por 2 previos antes de poder obtener la llave en común, es decir,

$$k' = a^{k_1} \text{ mód p}$$

De ahí y_1 va al individuo 2 y este le aplica su valor

$$k'' = k'^{k_2} \text{ mód p}$$

y el último individuo para poder encontrar la llave en común tendría que aplicar su llave:

$$k = k''^{k_3} \text{ mód p}$$

pero sustituyendo valores esto se convierte en

$$k = a^{k_1 * k_2 * k_3} \text{ mód p}$$

Y de esa forma podemos encontrar el valor en común

$$k = 15^{3*25*45} \text{ mód } 6833$$
$$k = 15^{3375} \text{ mód } 6833$$
$$k = 1765 \text{ mód } 6833$$

El valor en común para los tres individuos es:

$$k = 1765$$

3. Ejercicio 3

En un sistema RSA se sabe que $n = 153863$, $\varphi(n) = 153000$ y que la clave de cifrado es $e = 19$. Hallar la clave de decifrado.

Solución:

Necesitamos encontrar d, la cual necesita cumplir que

$$e * d \equiv 1 \text{ mód } \varphi(n)$$

es decir

$$19 * d \equiv 1 \text{ mód } 153000$$

y como se pide para RSA que $(e, \varphi(n)) = 1$ entonces existe solución.

Podemos reescribir como

$$19x - 153000y = 1 \tag{1}$$

Y usando el algoritmo de euclides

$$\begin{aligned} 153000 &= 19(8052) + 12 \\ 19 &= 12(1) + 7 \\ 12 &= 7(1) + 5 \\ 7 &= 5(1) + 2 \\ 5 &= 2(2) + 1 \\ 2 &= 2(1) \end{aligned} \tag{2}$$

Así,

$$\begin{aligned}
1 &= 5 - 2(2) \\
&= 5 - 2[7 - 5] \\
&= 5 + 2(5) - 2(7) \\
&= 5(3) - 2(7) \\
&= [12 - 7](3) - 2(7) \\
&= 3(12) - 3(7) - 2(7) \\
&= 3(12) - 5(7) \\
&= 3(12) - 5[19 - 12] \\
&= 3(12) - 5(19) + 5(12) \\
&= 8(12) - 5(19) \\
&= 8[153000 - 19(8052)] - 5(19) \\
&= 153000(8) - 19(8)(8052) - 5(19) \\
&= 153000(8) + 19(-64421)
\end{aligned} \tag{3}$$

Por lo que $x = -64421 \equiv 88579 \mod 153000$

De esta forma, la clave de decifrado es $d = 88579$