Laboratorio 1 Respuestas Parte 2

Presentado por:
Sara Nohemi Zavala (carné No. 18893)
Ricardo Antonio Valenzuela (carné No. 18762)
Jose Amado Garcia (carné No. 181469)
Juan Fernando De Leon Quezada (carné No. 17822)
Edgar Andree Toledo Torres (carné No. 18439)

Cifrado de la Información

Universidad del Valle de Guatemala

a. Obtener S4:
   i. Utilizando la ecuación matemática dada, ya que conocemos todas las variables de la misma, esto se puede calcular manualmente en calculadora.

$$1.\ X_{n+1} = (aX_n + c)\ mod\ m$$

   ii. 2148910388216139
b. Obtener S3 e incremento:
   i. Este proceso se divide en dos partes, en la primera parte nos enfocamos en conseguir el numero del incremento y en la segunda utilizamos este resultado para calcular el Step 3. Para conseguir el incremento debemos despejar este valor de la fórmula dada.

$$2.\ c = (X_{n+1} - aX_n)\ mod\ m$$

   Ya despejada la fórmula la podemos utilizar con los datos que sí conocemos, en este caso Xn+1 sería S2, el multiplicador, Xn sería S1 y m el módulo que estamos utilizando, para obtener el valor del incremento. Ya para conseguir el S3 solo debemos reemplazar los valores que conocemos y el recién sacado incremento en la ecuación matemática dada.
   ii. Incremento: 440065673588051
   iii. S3: 2316663380322452
c. Obtener S4, incremento, multiplicador:
   i. Este proceso fue mucho más complicado por que no cantábamos con el multiplicador, lo primero que se hizo fue delimitar 2 ecuaciones base:

$$S_2 = aS_1 + c\ mod\ m$$
$$S_3 = aS_2 + c\ mod\ m$$

   Con esto despejamos para c y las igualamos para tener una ecuación con datos que conocemos y una incógnita.

$$aS_1 - aS_2 = S_2 - S_3$$
$$a(S_1 - S_2) = S_2 - S_3\ mod\ m$$

   Nos pudimos percatar que para obtener la incognita debíamos obtener el inverso multiplicativo, utilizamos el algoritmo extendido de Euclides en conjunto con la Identidad de Bezout para sacar este dato que es el multiplicador.
   Ya con el valor del multiplicador hicimos los mismos pasos que en el ejercicio b para obtener el incremento, y por último se sacó S4 con la fórmula de siempre.
   ii. Multiplicador: 770741127604132
   iii. Incremento: 2015020420165804
   iv. S4: 1185433208698818