Segunda Tarea

Manuel Díaz Díaz y Gerardo Rubén López Hernández

May 7, 2022

1) Mostrar lo siguiente:
   a) Muestre que $a^2 \cong (-a)^2 \, mod(n)$.
   b) Demuestre que en $\mathbb{Z}_n$ $-a \cong (-1)a$.
   c) Dado un grupo cíclico demuestre que el problema del logaritmo discreto no depende de la raíz primitiva que se tome.

2) De los siguientes números cuales son primos, argumente mediante una prueba de primalidad: $n_1 = 67891234321234567897$, $n_2 = 13579246809876879657$ y $n_3 = 23192157311717657191$

3) El siguiente mensaje fue cifrado y firmado mediante el algoritmo RSA, el cifrado fue implementado pasando los caracteres que están entre el rango de valores $[33, 125]$ en ascii, el cifrado tiene los siguientes parámetros:$(837209, 61)$

   232723 371533 216667 785056 316903 785056 679163 24385 679163 371533 482793 515822 24385 216667 406281 637099 229117 24385 482793 494014 371533 679163 371533 482793 316903 785056 581471 229117 24385 229117 371533 216667 243970 371533 704420 482793 24385 703849 371533 803021 254817 482793 278695 371533 229117 406281 704420 406281 482793 371533 494014 371533 90930 24385 515822 24385 316903 406281 243970 278695 216667 785056 316903 24385 679163 406281 243970 236773 316903 90930 406281 278695 406281 229117 475793 236773 371533 216667 406281 278695 236773 482793 371533 482793 371533 704420 316903 785056 216667 216667 406281 803021

   a) Mediante el algoritmo de criba cuadrática encuentra la descomposición de $n = 837209$ (solo pon las relaciones que te llevan a la solución, la base y las cotas M y B).
   b) Dar e^{-1}.
   c) Descifrar el mensaje.
   d) Con a el último carácter que es primo relativo con $\varphi(n)$ y x es el carácter previo de a cifrados, determina la firma correcta $f_1 = 759181$ o $f_2 = 489650$ haga la verificación de firma.

4) El siguiente mensaje cifrado se elaboro con el algoritmo Gammal con parámetros $(977, 53, 13)$, los caracteres están en código ascii en el intervalo $[33, 125]$:

   (855,238) (413,633) (9,258) (954,424) (834,546) (682,233) (694,460) (26,409) (245,230) (799,938) (579,221) (409,352) (346,161) (897,714) (969,618) (747,617) (783,806) (441,382) (778,811)

a) Mediante el algoritmo de cálculo de índices encuentre $a = log_{53}(13)$, con la base $B = \{2, 3, 5, 7, 11\}$ incluya las ecuaciones con las que se obtiene el resultado, incluyendo los valores de los índices involucrados.

b) El mensaje fue firmado con el algoritmo de Gammal con parámetros $(977, 53, a, 13)$ donde a es la llave privada anterior. El último carácter del cifrado que cumple las condiciones de la K en la firma de Gammal es k y x el valor previo a k en el mensaje cifrado. Tanto k como x se encuentran en la segunda coordenada del mensaje cifrado. La firma es $(258, 280)$, haga el proceso de verificación y dictamine si la firma es valida.