Segunda Tarea.

Manuel Díaz Díaz, José Canek Aguilar García y Gerardo Rubén López Hernández

May 11, 2020

1) Mediante el algoritmo de ro-Pollar descomponer el número $n = 557437$, expresando claramente el proceso.

2) Sea $\mathbb{Z}_{10007}$ y $S = \{2, 3, 5, 7\}$ calcular el índice de $\beta = 9451$ en $\alpha = 5$.

   a) Mostrar que $\alpha = 5$ es raíz primitiva de $\mathbb{Z}^*_{10007}$.

   b) $\rho_1 = 4063$, $\rho_2 = 5136$ y $\rho_0 = 9865$, uselos para calcular los logaritmos de $2, 3$ y 7 base 5, ¿porqué no es necesario calcular el logaritmo de 5 base α?

   d) Dados los cálculos anteriores obtener el índice de $\beta = 9451$ en α módulo 10007.

3) Descifrar el siguiente mensaje en RSA con parámetros $(2257, 7)$ con las siguientes condiciones:

3i) Aplicar el algoritmo de criba cuadrática para descomponer a 2257.

   a) Usar la siguiente base $S = \{-1, 2, 3, 17\}$.

   b) Dar M, B y decir para que sirven.

   c) Expresar el proceso claramente por el cual se obtienen x e y, con los cuales se puede descomponer 2257.

   d) Dar los valores para los cuales se obtienen x e y tales que
   $(x - y, 2257)$ es un factor no trivial de 2257.

3ii) Descifrar el mensaje mediante el siguiente proceso:

a) Dar las llaves pública y privada de RSA y su proceso de como se obtienen de manera resumida pero clara.

b) Descifrar el mensaje.

585 1660 585 2011 431 322 431 322 274 585 322 431 585 1660 68 322 1660 1933 1132 128 1995 322 2218 322 128 399 585 1660 128 399 322 585 2011 1933 1132 1411 2011 585 1660 128 399 233 233 322 2218 585 274 319 2011 585 1660 128 399 233 233 319 1660 319 2011 399 68 1660 399 1387 399 128 322 274 322 2218 399 2187 319 2011 399 68 1660 399 1387 399 128 322 585 1660 585 2011 431 585 128 322 2011 319 1418 1132 585 2011 322 233 585 128 319 1660 233 319 1 322 2011 399 128 319 1411 322 284 585 274 322 1660 1418 1132 585 585 2011 431 319 585 2011 431 322 1933 1132 1411 2187 399 284 585 274 431 399 2187 319

Sugerencia el polinomio $q(x)$ no sobre pasa $x = \pm 27$.