Segunda Tarea.

Manuel Díaz Díaz y Gerardo Rubén López Hernández

December 7, 2020

1) Sean $p = 163$ y $\alpha = 3$.

   a) Mostrar que α es raíz primitiva.

   b) De todas las raíces primitivas.

2) Logaritmo discreto realice lo que se pide a continuación.

   a) Mediante el algoritmo de paso grande paso chico encontrar el logaritmo de 19 base α explicar detalladamente como se llega al resultado.

   b) Con el algoritmo de Pohling Hellman calcular $log_3(19)$, desarrolle su procedimiento como en los ejercicios anteriores.

   c) Dada la base $B = \{2, 3, 5, 7, 11\}$ encontrar $log_3(19)$. Explique claramente el proceso. De su opinion cual de los métodos se le facilito mas.

3) Descifrar el siguiente mensaje cifrado en Gammal con parámetros $G(163, 3, 19)$, los caracteres están cifrados en código ascii del 65 al 90, la ñ se tomo como n.

   (7,27) (7,75) (7,125) (7,38) (5,108) (5,137) (7,12)(7,151)(7,153)(7,25)(11,80)

   (7,90)(5,152)(7,101)(7,88)(2,5)(5,115)(11,23)(5,123).

4) Sea $n = 23999$ Mediante el algoritmo se Solovay-Strassen decir si n es primo. Explique claramente.

5) Descomponer a n con el algoritmo rho de pollard. Explicar detalladamente.

6) Hacer lo mismo con el algoritmo rho-1. Explicar detalladamente.

7) Mostrar que para los números 2,5,13, y 73 el númeo $n = 23999$ es un residuo cuadrático.

8) Aplicar el algoritmo de la criba cuadrática a $n = 23999$ para descomponer n.

   a) Dar las cotas M y B y decir para que sirve cada una

   b) Dada la base $B = \{-1, 2, 5, 13, 73\}$ expresa claramente como se obtienen x e y tales que $(x - y, n) = d$ donde d es un factor no trivial de n.

   c) Dar $157^{-1} mod(\varphi(n))$.

d) Descifrar el mensaje en RSA con parámetros $(23999, 157)$. En esta ocasión la codificación de los caracteres es módulo 26 y la ñ se toma como n.

10473 17984 11552 10435 19226 11552 10435 22142 3933 22173 17984 14264 12386 14264 10227 352 19226 10227 17984 10227 19226 2774 14264 10491 594 15396 10227 19226 17802 594 12897 19226 12897 5137 2774 14264 10491 594 11552 14264 3933 17802 19226 11552 19226 11552 594 22142 10227 14264 3933 14264 10227 11552 22142 10473 17768 19226 10227 594 19226 12897 14264 3933 17984 3933 3933 14264 2460 14264 3933 22173 17984 14264 2460 594 12897 22142 3933 10491 14264 3933 19226 17768 2460 14264 11552 594 19226 10473 22142 3933 3933 17984 3933 17768 2460 22142 2774 14264 3933 22142 2460 14264 3933