Segunda tarea de criptografía y seguridad

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

14 de abril de 2019

1) Sea $\mathbb{Z}_{89627}$.

   a) Muestre que 2 es generardor de $\mathbb{Z}^*_{89627}$.

   b) Mediante cálculo de índices encontrar $log_2(88777)$.

   c) Mediante paso grande paso chico encontrar $log_2(88777)$.

   e) Mediante rho- Pollard para logaritmos encontrar $log_2(88777)$.

   f) Con el método de su preferencia calcular $log_2(54539)$.

   g) Si los parámetros públicos son $(89627, 2, 88777)$, descifrar el siguiente mensaje el cual está encriptado con Gamal justifica tu desifrado.
   Si $\gamma = 54539$

$(\gamma, 81315)(\gamma, 87570)$	$(\gamma, 31275)(\gamma, 35473)$	$(\gamma, 25020)$
$(\gamma, 18765)(\gamma, 50040)$	$(\gamma, 31275)(\gamma, 50040)$	$(\gamma, 12510)$
$(\gamma, 50040)(\gamma, 68805)$		

2) Sea $n = 475,743,576,304,725,019$.(el número está separado por comas para una mejor lectura).

   a) Descomponer n con el algoritmo de la criba cuadrática.

   b) Cálcular $\phi(n)$ y descomponerla como producto de potencias de primos.

   c) Mostrar que $(257, \phi(n-1)) = 1$.

   d) Encontrar d tal que $d(257) \cong 1 mod(\phi(n-1))$.

   e) Si la llave pública es $(n, 257)$ descifrar el siguiente mensaje:
   57405399740998460
   221672271139134806
   999859790124261
   409459118544434045
   69264543019213165
   36113359812750643
   102787661370136461
   320963384754703589
   409459118544434045
   221672271139134806
   422003967026332448

3) a) Mostrar que el problema del logaritmo discreto no depende del generador.

   b) Sea $n = 10942095573514557503$ decir si es primo o compuesto en caso de ser compuesto descomponerlo.(usando métodos vistos en clase).