Segunda Tarea

Manuel Díaz Díaz, Gerardo R. L.H. Canek Aguilar.

October 31, 2022

Nota: Todos los cifrados han sido codificados en unicode. En el caso de entregar código fuente deben ser con: Nombres de programadores o programador (solo nombre de personas involucradas en la programación) fecha de elaboración, comentado en cada módulo y deben expresar que son tareas.

Descifrados sin llaves privadas no cuentan.

Tiempo de resolución de tarea a lo mas una hora (partiendo de que han programado los algoritmos, es decir programen lo mas que puedan).

1) Dado el siguiente número $n = 1,148,289,976,600,001$ aplique una prueba de primalidad en la cual se ocupe testigo (testigo de Fermat,testigo de Euler,testigo fuertes,...) y cite cual es.

   a) Determina si el número $n = 1,148,289,976,600,001$ es primo con una prueba de primalidad probabilística vista en clase. Para el caso de ser primo explique como llega a tal conclusión.

   b) En caso de ser compuesto de explícitamente la iteración y su testigo determina que es compuesto.

2) Mediante el algoritmo de ro de Pollard para enteros descomponga $n = 7784099$

a) De la función semialeatoria empleada

b) Número de iteración en el cual fue exitoso el algoritmo y factor encontrado.

c) Descifre el siguiente mensaje RSA, el cual esta en unicode:
   Llave públicaRSA=(7784099 , 7), mensaje cifrado= 6308199
   Llave públicaRSA=(7784099 , 11), mensaje cifrado= 5536286
   Llave públicaRSA=(7784099 , 13), mensaje cifrado= 159060
   Llave públicaRSA=(7784099 , 19), mensaje cifrado= 6724396
   Llave públicaRSA=(7784099 , 23), mensaje cifrado= 26176
   Llave públicaRSA=(7784099 , 29), mensaje cifrado= 1117219
   Llave públicaRSA=(7784099 , 37), mensaje cifrado= 6925326
   Llave públicaRSA=(7784099 , 43), mensaje cifrado= 7550806
   Llave públicaRSA=(7784099 , 47), mensaje cifrado= 1525454
   Llave públicaRSA=(7784099 , 49), mensaje cifrado= 4142333

3) Mediante e algoritmo de la criba cuadrática descomponga $n = 4245221$ y descifre el mensaje en RSA que se proporciona mas adelante.

a) De las cotas de base e intervalo, escriba la base

b) Proporcione las i de $q(i)$ con las cuales se obtiene la solución, x, y tales que $(x-y, n) = d$ donde de es un factor primo de n, describa de manera clara y metódica como obtiene y.

c) Descifre el siguiente mensaje cifrado en RSA:
Llave públicaRSA=(4245221 , 7), mensaje cifrado= 2787825
Llave públicaRSA=(4245221 , 11), mensaje cifrado= 2055284
Llave públicaRSA=(4245221 , 13), mensaje cifrado= 2061537
Llave públicaRSA=(4245221 , 17), mensaje cifrado= 4003203
Llave públicaRSA=(4245221 , 19), mensaje cifrado= 3833015
Llave públicaRSA=(4245221 , 23), mensaje cifrado= 504464
Llave públicaRSA=(4245221 , 29), mensaje cifrado= 1181333
Llave públicaRSA=(4245221 , 31), mensaje cifrado= 3063352
Llave públicaRSA=(4245221 , 37), mensaje cifrado= 1145481
Llave públicaRSA=(4245221 , 41), mensaje cifrado= 899155
Llave públicaRSA=(4245221 , 43), mensaje cifrado= 1046164
Llave públicaRSA=(4245221 , 47), mensaje cifrado= 1315170
Llave públicaRSA=(4245221 , 49), mensaje cifrado= 1878863
Llave públicaRSA=(4245221 , 53), mensaje cifrado= 2088416
Llave públicaRSA=(4245221 , 59), mensaje cifrado= 2571920
Llave públicaRSA=(4245221 , 61), mensaje cifrado= 2621019
Llave públicaRSA=(4245221 , 71), mensaje cifrado= 1550905

d) verifique si la firma digital RSA $firma = 1107437$ del mensaje $m = 1550905$ con parámetros $(4245221, 7)$ es valida.

4) El siguiente mensaje fue cifrado con el algoritmo de Gammal con llave pública $= (2011, 17, 19)$, mediante el algoritmo de cálculo de índices con la base $B = \{2, 3, 5, 7, 11\}$ encuentre el índice de 19 base 17 módulo 2011.

a) De las ecuaciones ya solucionadas para cada índice

b) De la iteración en la cual se obtiene el índice de 19 base 17 módulo 2011.

c) Descifre el mensaje: (891 , 260),(1070 , 1838), (91 , 934), (1547 , 1835), (156 , 761), (641 , 1542), (842 , 1820), (237 , 1757), (7 , 1215), (119 , 1898)

d) Verifique la siguiente firma digital Gammal $s_k(33, 7) = (\gamma = 156, \delta = 477)$, con llave pública $= (2011, 17, 19)$ ¿Es valida la firma?