Universidad Nacional Autónoma de México

FACULTAD DE CIENCIAS

Criptografía y Seguridad

Tarea 2

Cifrados de Clave Pública

Profesor:

Manuel Díaz Díaz

Integrantes:

Lázaro Pérez David Jonathan

Licona Gómez Aldo Daniel

Marín Parra José Guadalupe de Jesús

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 cuál 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.

   Solución. Gracias al siguiente código en python pudimos llegar a la respuesta.

```
from random import randint

def Test_Fermat(n,k):
    '''
    Prueba de primalidad de Fermat
    param n: Numero a probar
    param k: Numero de iteraciones, mas iteraciones
    equivale a mayor precision y complejidad de tiempo
    return: Verdadero si el numero es probablemente
    primo, de lo contrario Falso.
    '''
    num = 0

    if n < 4:
        return n == 2 or n == 3

    for _ in range(k):
        num = num+1
        print(f'Iteacion numero:{num}')
        print(f'Testigo de Fermat para la composicion de {n}')
        a = randint(2, n - 2)

        print(pow(a, n - 1, n))

        if pow(a, n - 1, n) != 1:
            print("FALSE")
            print()
        if pow(a, n - 1, n) != 1 and num == k:
                return False

    return True

print(Test_Fermat(1148289976600001,10))
```

Con el cual obtenemos el siguiente resultado.

```
Iteacion numero:1
Testigo de Fermat para la composicion de 1148289976600001
376223426613442
FALSE

Iteacion numero:2
Testigo de Fermat para la composicion de 1148289976600001
490178616878212
FALSE

Iteacion numero:3
Testigo de Fermat para la composicion de 1148289976600001
927165513118241
FALSE

Iteacion numero:4
Testigo de Fermat para la composicion de 1148289976600001
319159446554282
FALSE

Iteacion numero:5
Testigo de Fermat para la composicion de 1148289976600001
535070638200061
FALSE

Iteacion numero:6
Testigo de Fermat para la composicion de 1148289976600001
1069031494917211
FALSE

Iteacion numero:7
Testigo de Fermat para la composicion de 1148289976600001
91999188253320
FALSE

Iteacion numero:8
Testigo de Fermat para la composicion de 1148289976600001
226273754629075
FALSE

Iteacion numero:9
Testigo de Fermat para la composicion de 1148289976600001
36334933377583
FALSE

Iteacion numero:10
Testigo de Fermat para la composicion de 1148289976600001
168121264587203
FALSE
```

En un programa que aplica el Test de Fermat se da el numero 1148289976600001 y se le aplica el test 10 veces a las cuales a cada una se obtiene un testigo de Fermat para la composicion de 1148289976600001 ademas de que no se cumple que $a^{p-1} = 1 \ mod \ p$. En las 10 iteraciones se regresa un FALSE por lo que el numero 1148289976600001 no es primo, es decir, es un numero compuesto.

2. Mediante el algoritmo rho de Pollard para enteros descomponga $n = 7784099$.

   a) De la función semialeatoria empleada.
   Solución. $g(x) = (x^2 + 1) \ mod \ n$

   b) Número de iteración en el cual fue exitoso el algoritmo y factor encontrado.
   Solución. Gracias a la implementación del siguiente código en python pudimos encontrar la solución.

```
import sys;
#Valor el cual vamos a descomponer
valor = 7784099

#Si la longitud es mayor a 1 entonces asignamos el valor
if (len(sys.argv) > 1):
        valor = int(sys.argv[1])

#Funcion que devuelve el Maximo Comun Divisor
def mcd(x,y):
        if y == 0:
                return x
        else:
                return mcd(y,x%y)

#Funcion con la cual verificamos si un numero es primo
def funcion(x,n):
        return (x*x+3) % n

#Funcion con la cual definimos el algoritmo rho de pollard
```

```
def pollard(a):
        print ("A B MCD")
        x = 2
        y = 2
        d = 1
        while d == 1:
                x = funcion(x,a)
                y = funcion(funcion(y,a,),a)
                d = mcd(abs(x-y),a)
                print (x,y,d)
                if d > 1 and a > d:
                        return d
                if d == a:
                        return -1

#Imprimimos el resultado con una cadena
print ("El primer factor es: " + str(pollard(valor)))
```

Con lo cual obtenemos el siguiente resultado.

```
→ Tarea2 git:(main) ✗ python3 rho.py
A B MCD
7 52 1
52 7327852 1
2707 1845174 1
7327852 5063956 1
6733653 7219360 1
1845174 4676266 1
3380966 5664235 1
5063956 2418595 1
2636002 1318906 1
7219360 4221604 1
33896 3267394 1
4676266 7197052 1
6939306 3203910 1
5664235 4806881 1
753007 2063578 1
2418595 6022397 1
7057508 4593270 1
1318906 3836582 1
433309 186558 1
4221604 2309648 1
4365250 2914470 1
3267394 3460287 1
2909135 449984 1
7197052 3539869 1
6549284 3846982 1
3203910 1769574 1
38922 707536 1
4806881 3852499 1
3431336 6234147 1
2063578 1328139 1
531345 1165666 1
6022397 5123308 1
3608616 594496 1
4593270 4344473 1
6170016 3651842 1
```

```
3836582 1848118 1
3870479 2708565 1
186558 835104 1
1180738 5754880 1
2309648 465788 1
7486910 2664633 1
2914470 3138393 1
2006519 2299604 1
3460287 5754791 1
7199582 1868657 1
449984 5508614 1
5617071 3582602 1
3539869 3794805 1
1217142 3248046 1
3846982 1788032 1
1375745 1467591 1
1769574 935867 1
4795759 6480821 1
707536 2611404 1
4000510 2552797 1
3852499 1314574 1
1584179 2429847 1
6234147 3526247 1
7000729 1217352 1
1328139 872087 1
6313033 4304317 1
1165666 1247415 1
470317 1233313 1
5123308 886766 1
7239105 5840081 1
594496 4755684 2789
El primer factor es: 2789
```

Por lo cual el factor encontrado fue 2789 en la iteración número 66.

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
Solución. Gracias a la implementación del proyecto 2, tenemos que la palabra decifrada es ”ES-RUTINA.”

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

a) De las cotas de base e intervalo, escriba la base.
Solución. Para que podamos obtener la base, debemos proponer números primos, en este caso haremos una lista como la que sigue.

$$L = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...\}$$

Buscamos números primos P que cumplan con la propiedad: $\frac{N}{P} = 1$ en donde la N es el modulo, es decir, $N = 4245221 \ mod \ P = 1$ los cuales consideraremos valores validos para obtener la base.
Los primeros dos primos se incluyen al iniciar por lo que empezamos con el 5 y aplicamos el criterio de Euler, quedando de la siguiente manera.

$$4245221^2 \equiv -1(mod\ 5)$$

Entonces tenemos que el 5 es válido para N, por lo que lo agregaremos, continuamos con el mismo proceso hasta obtener varios primos.

$$\begin{gathered} 4245221^2 \equiv 1(mod 5) \text{ se agrega} \\ 4245221^3 \equiv 1(mod 7) \text{ se agrega} \\ 4245221^5 \equiv -1(mod 11) \text{ no se agrega} \\ 4245221^6 \equiv -1(mod 13) \text{ no se agrega} \\ 4245221^8 \equiv 1(mod 17) \text{ se agrega} \\ 4245221^9 \equiv -1(mod 19) \text{ no se agrega} \end{gathered}$$

Entonces nuestra lista de primos queda como sigue, tomando en cuenta que -1 y 2 están agregados

$$L = \{-1, 2, 5, 7, 17, 31, 37, 41\}$$

b) Proporcione las i de $q(i)$ con las cuales se obtiene la solución, x, y tales que $(x - y, n) = d$ donde d es un factor primo de n, describa de manera clara y metódica como obtiene y.
Solución. Tenemos que $m = \sqrt{4245221} = 2060$ con los elementos $i = t + 1 = 9$
Entonces creamos una tabla que queda de la siguiente manera.

i	x	$q(x)$	Factores	a_i	Vectores
1	1	2500	$2^2 * 5^4$	2061	(0,0,0,0,0,0,0,0)
3	-1	-5740	$-1 * 2^2 * 5 * 7 * 41$	2059	(1,0,1,1,0,0,0,1)
2	4	14875	$5^3 * 7 * 17$	2064	(0,0,1,1,1,0,0,0)
4	39	160580	$2^2 * 5 * 7 * 31 * 37$	2099	(0,0,1,1,0,1,1,0)
5	76	317275	$5^2 * 7^3 * 31$	2136	(0,0,0,1,0,0,1,0)
6	-129	-516460	$-1 * 2^2 * 5 * 7^2 * 17 * 31$	1931	(1,0,1,0,1,1,0,0)
7	-146	-581825	$-1 * 5^2 * 17 * 37^2$	1914	(1,0,0,0,1,0,0,0)
8	-183	-722092	$-1 * 2^2 * 7 * 17 * 37 * 41$	1877	(1,0,0,1,1,0,1,1)
9	-316	-1203685	$-1 * 5 * 7^2 * 17^3$	1744	(1,0,1,0,1,0,0,0)

Por lo que tenemos que $V_4, V_5, V_6, V_7 = 0$
Ahora tenemos que calcular x, quedando $x = 2099 \cdot 2136 \cdot 1931 \cdot 1914 (mod\ 4245221) =$ 3645026.
Después obtenemos los exponentes de cada número primo.
$e_1 = 1$ $e_2 = 2$
$e_3 = 3$ $e_4 = 3$
$e_5 = 1$ $e_6 = 1$
$e_7 = 2$ $e_8 = 0$
Ahora tenemos que calcular y, quedando $y = -1 \cdot 2^2 \cdot 5^3 \cdot 7^3 \cdot 17 \cdot 31 \cdot 37^2 \cdot 41^0 (mod\ 4245221) =$ 306766.
A continuación tenemos que $MCD(x - y, n) = MCD(3338260, 4245221) = 2011$
Por lo que ahora tenemos ambos factores de n y el resultado queda como sigue.
$\frac{4245221}{2011} = 2111.$

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
Solución. Gracias a la implementación del proyecto 2, tenemos que la palabra decifrada es ”¡BIEN-DESCIFRADO!”

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

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.
Solución. Nuestro sistema de ecuaciones fue:
$4log_{17}(3) + log_{17}(11) = 891$
$log_{17}(2) + log_{17}(3) + log_{17}(5) + 2log_{17}(7) = 1270$
$2log_{17}(2) + log_{17}(3) = 12$
$log_{17}(2) + log_{17}(3) + log_{17}(5) = 30$
$log_{17}(2) + log_{17}(3) + log_{17}(11) = 66$

Resolvemos con Gauss-Jordan y nos da:

$log_{17}(2) = -\frac{789}{7}$
$log_{17}(3) = \frac{1662}{7}$
$log_{17}(5) = -\frac{663}{7}$
$log_{17}(7) = 1440$
$log_{17}(11) = -\frac{411}{7}$

b) De la iteración en la cual se obtiene el índice de 19 base 17 módulo 2011.
Solución.
Tomamos una k aleatoria = 54

Entonces tenemos que 19 . 17^{54} mod 2011 = 567 = 3^4 x 7

Como si es factoriable en B

Entonces $log_{17}(19) = (4log_{17}(3) + log_{17}(7) - 54)$ mod 2010 = 1958.2378686437537

En el indice 739 tenemos que 17^{739} mod 2011 = 19

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

d) Verifique la siguiente firma digital Gammal $s_k = (33, 7) = (\gamma = 156, \delta = 477)$, con llave pública = (2011, 17, 19) ¿Es válida la firma?
Solución. $Sig_k(x) = Sig_k(1550905)\ 1550905^1 211743\ (mod\ 4245221) = 1107437\ 1550905 \equiv 1107437^7\ (mod\ 4245221) \rightarrow 1550905 \equiv 1550905\ (mod\ 4245221)$