Tarea 2
Criptografía

Emmanuel Peto Gutiérrez Lisandro Vázquez Aguilar

Diciembre 2020

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

   a) Mostrar que α es raíz primitiva.

   Solución:

   Se define el periodo de b módulo n como el número per más pequeño tal que $b^{per} \cong 1$ mód n.

   Se tiene que $\Phi(163) = 162 = (2)(3)(3)(3)(3)$, y como 3 es primo relativo con 163 entonces el periodo de 3 módulo 163 debe dividir a 162. Si el periodo es menor a 162 significa que 3 no es raíz, en otro caso sí es raíz. Hay que ver si alguno de los divisores d de 162 con $d < 162$ cumplen que $3^d \cong 1$ mód 163.

   $3^2 \cong 9$ mód 163
   $3^3 \cong 27$ mód 163
   $3^6 \cong 77$ mód 163
   $3^9 \cong 123$ mód 163
   $3^{18} \cong 133$ mód 163
   $3^{27} \cong 59$ mód 163
   $3^{54} \cong 58$ mód 163
   $3^{81} \cong 162$ mód 163
   $3^{162} \cong 1$ mód 163

   Se tiene que ningún divisor de 162 menor que 162 es congruente con 1 módulo 163, lo que significa que el periodo es 162 y por lo tanto 3 es una raíz primitiva. De hecho, se puede comprobar que 3 es raíz primitiva generando todo el conjunto $\mathbb{Z}^*_{163}$.

   Se da una lista de pares ($potencia$, $residuo$), donde $3^{potencia} \cong residuo$ mód 163.

   (162,1), (77,2), (1,3), (154,4), (21,5), (78,6), (113,7), (69,8), (2,9), (98,10), (55,11), (155,12), (39,13), (28,14), (22,15), (146,16), (15,17), (79,18), (67,19), (13,20), (114,21), (132,22), (45,23), (70,24), (42,25), (116,26), (3,27), (105,28), (139,29), (99,30), (129,31), (61,32), (56,33), (92,34), (134,35), (156,36), (111,37), (144,38), (40,39), (90,40), (8,41), (29,42), (10,43), (47,44), (23,45), (122,46), (50,47), (147,48), (64,49), (119,50), (16,51), (31,52), (72,53), (80,54), (76,55), (20,56), (68,57), (54,58), (27,59), (14,60), (12,61), (44,62), (115,63), (138,64), (60,65), (133,66), (143,67), (7,68), (46,69), (49,70), (118,71), (71,72), (19,73), (26,74), (43,75), (59,76), (6,77), (117,78), (25,79), (5,80), (4,81), (85,82), (86,83), (106,84), (36,85), (87,86), (140,87), (124,88), (107,89), (100,90), (152,91), (37,92), (130,93), (127,94), (88,95), (62,96), (52,97), (141,98), (57,99), (34,100), (125,101), (93,102), (95,103), (108,104), (135,105), (149,106), (101,107), (157,108), (161,109), (153,110), (112,111), (97,112), (38,113), (145,114), (66,115), (131,116), (41,117), (104,118), (128,119), (91,120), (110,121), (89,122), (9,123), (121,124), (63,125), (30,126), (75,127), (53,128), (11,129), (137,130), (142,131), (48,132), (18,133), (58,134), (24,135), (84,136), (35,137), (123,138), (151,139), (126,140), (51,141), (33,142), (94,143), (148,144), (160,145), (96,146), (65,147), (103,148), (109,149),

(120,150), (74,151), (136,152), (17,153), (83,154), (150,155), (32,156), (159,157), (102,158), (73,159), (82,160), (158,161), (81,162)

b) Dé todas las raíces primitivas.

Solución:

Para resolver este problema se usó ayuda de un programa en Python que calcula el periodo de b módulo n. Esto es, el número más pequeño *per* tal que $b^{per} \cong 1 \mod n$. Si el periodo de b es $n-1$, significa que b es raíz primitiva. Así, sólo hay que iterar b de 2 a $n-1$ para encontrar todas las raíces primitivas.

Raíces:

2, 3, 7, 11, 12, 18, 19, 20, 29, 32, 42, 44, 45, 50, 52, 63, 66, 67, 68, 70, 72, 73, 75, 76, 79, 80, 82, 89, 92, 94, 101, 103, 106, 107, 108, 109, 112, 114, 116, 117, 120, 122, 124, 128, 129, 130, 137, 139, 147, 148, 149, 153, 154, 159.

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 cómo se llega al resultado:

Primero se elige $m = \sqrt{163} = 13$. Se calcula $3^i \mod 163$ con $1 \leq i \leq 13$. Se toma $r = b^i \mod 163$

i	1	2	3	4	5	6	7	8	9	10	11	12	13
r	3	9	27	81	80	77	68	41	123	43	129	61	20

Ahora se ordenan las r's.

i	1	2	13	3	8	10	12	7	6	5	4	9	11
r	3	9	20	27	41	43	61	68	77	80	81	123	129

Como el 19 no está en la tabla hay que seguir iterando. Se calcula $\alpha^{-1} = 109 \mod 163$.

$19(3^{-13}) \mod 163 = 58$, $19(3^{-26}) \mod 163 = 117$, $19(3^{-39}) \mod 163 = 14$, $19(3^{-52}) \mod 163 = 17$, $19(3^{-65}) \mod 163 = 9$. Como 9 sí está en la tabla ya acabó el algoritmo.

Entonces $19 = 3^{5 \cdot 13} \cdot 3^2$ y el logaritmo base 3 de 19 es $5 \cdot 13 + 2 = 67$.

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

El orden del grupo es 162, y la factorización de 162 es 2×3^4. Sea $x = \log_3(19)$, $x_i = x \mod p_i^{e_i}$.

Hay que calcular $x_1 = x \mod 2$. Se calcula $\bar{\alpha} = \alpha^{n/2} \mod 163 = 3^{81} \mod 163 = 162$. Luego, $\bar{\beta} = 19^{81} \mod 163 = 162$.

$\ell_0 = \log_{\bar{\alpha}}(\bar{\beta}) = \log_{162}(162) = 1$. Así que $x_1 = 1$.

Ahora hay que calcular $x_2 = x \mod 3^4 = \ell_0 + 3\ell_1 + 3^2\ell_2 + 3^3\ell_3$.

$\bar{\alpha} = \alpha^{n/3} \mod 163 = 3^{54} \mod 163 = 58$. Se tiene que $\gamma = 1, \gamma^{-1} = 1$, $\bar{\beta} = (\beta\gamma^{-1})^{n/3} \mod 163 = 19^{54} \mod 163 = 58$.

$\ell_0 = \log_{\bar{\alpha}}(\bar{\beta}) = \log_{58}(58) = 1$.

Ahora se va a calcular ℓ_1

$\gamma \leftarrow \gamma\alpha^{\ell_0 \times 3^0} \mod 163 = 3^1 \mod 163 = 3$. $\gamma^{-1} = 109$. $\bar{\beta} = (\beta\gamma^{-1})^{n/3^2} = (19 \times 109)^{18} \mod 163 = 58$.

$\ell_1 = \log_{\bar{\alpha}}(\bar{\beta}) = \log_{58}(58) = 1$.

Se calcula ℓ_2

$\gamma \leftarrow \gamma\alpha^{\ell_1 \times 3^1} \mod 163 = 3 \times 3^3 \mod 163 = 81$.

$\gamma^{-1} = 161$

$\bar{\beta} = (\beta\gamma^{-1})^{n/3^3} \mod 163 = (19 \times 161)^6 \mod 163 = 58$
$\ell_2 = \log_{\bar{\alpha}}(\bar{\beta}) = \log_{58}(58) = 1$
Se calcula ℓ_3
$\gamma \leftarrow \gamma\alpha^{\ell_2 \times 3^2} \mod 163 = 81 \times 3^9 \mod 163 = 20$
$\gamma^{-1} = 106$
$\bar{\beta} = (\beta\gamma^{-1})^{n/3^4} \mod 163 = (19 \times 106)^2 \mod 163 = 104$
$\ell_3 = \log_{\bar{\alpha}}(\bar{\beta}) = \log_{58}(104) = 2$
Finalmente hay que calcular x_2
$x_2 = 1 + 3(1) + 3^2(1) + 3^3(2) = 67.$
Se tiene el sistema de congruencias:
$x \cong 1 \mod 2$
$x \cong 67 \mod 81$

Usando el teorema chino del residuo se puede encontrar la solución única. Sea $M = 2 \times 81 = 162$, $M_1 = M/2 = 81$, $M_2 = M/81 = 2$. Sea s_i el inverso multiplicativo de M_i. Se tiene que $s_1 = 1$ y $s_2 = 41$, ya que $M_1 s_1 \mod 2 = 81(1) \mod 2 = 1$ y $M_2 s_2 \mod 81 = 2(41) \mod 81 = 1$.

La solución es: $x = a_1 s_1 M_1 + a_2 s_2 M_2 \mod M = 1(1)81 + 67(41)(2) \mod 162 = 5575 \mod 162 = 67$.

Por lo tanto $\log_3(19) = 67 \mod 163$

c) Dada la base B = 2, 3, 5, 7, 11 encontrar $log_3(19)$. Explique claramente el proceso.

Eligiendo $k \in \{21, 49, 56, 135, 154\}$

Se tienen las siguientes relaciones:
$3^{21} \cong 5 \mod 163$
$3^{49} \cong 70 = 2 \times 5 \times 7 \mod 163$
$3^{56} \cong 33 = 3 \times 11 \mod 163$
$3^{135} \cong 105 = 3 \times 5 \times 7 \mod 163$
$3^{154} \cong 4 = 2^2 \mod 163$

Aplicando logaritmos, el sistema de ecuacions que se obtiene es el siguiente:

n,log	$\log_3(2)$	$\log_3(3)$	$\log_3(5)$	$\log_3(7)$	$\log_3(11)$
21	0	0	1	0	0
49	1	0	1	1	0
56	0	1	0	0	1
135	0	1	1	1	0
154	2	0	0	0	0

Como la base es 3, se tiene que $\log_3(3) = 1$.
Luego, $2\log_3(2) \cong 154 \mod 163$, entonces $\log_3(2) = 77 \mod 163$.
$\log_3(5) = 21 \mod 163$.
$\log_3(3) + \log_3(7) \cong 114 \mod 163$, y como $\log_3(3) = 1$ se tiene que $\log_3(7) \cong 113 \mod 163$.
$\log_3(3) + \log_3(11) \cong 56 \mod 163$. Como $\log_3(3) = 1$ se tiene que $\log_3(11) \cong 55 \mod 163$.
Ahora se elige $k = 43$.
$\beta\alpha^k = 19 \times 3^4 3 \cong 121 = 11^2 \mod 163$.
De modo que $\log_3(19) = 2\log_3(11) - 43 = 2(55) - 43 = 67 \mod 163$.

Dé su opinion cual de los métodos se le facilitó más.

El método más fácil es el de paso chico paso grande pues, aunque puede necesitar más pasos, es más intuitivo de ejecutar. El algoritmo de Pohling Hellman requiere resolver el problema de factorización y el de cálculo de índices requiere verificar si un sistema de ecuaciones es linealmente independiente.

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.

   Las entradas son de la forma (a, b)

   (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).

   Supóngase que la llave pública es $y = 19$. Se sabe que $19 = 3^x \mod 163$, y por el ejercicio anterior se tiene que $x = 67$, que es la llave secreta. Ahora, para encontrar el mensaje se debe calcular $M = b/a^x$ para cada par (a, b). En realidad hay que multiplicar b por el inverso multiplicativo de a^x módulo 163 para obtener M. En las siguientes tablas se resumen los cálculos.

a	b	a^x	a^{-x}	$M = b \times a^{-x} \mod 163$
7	27	50	75	69
7	75	50	75	83
7	125	50	75	84
7	38	50	75	79

5	108	37	141	69
5	137	37	141	83
7	12	50	75	85
7	151	50	75	78
7	153	50	75	65

7	25	50	75	82
11	80	124	117	69
7	90	50	75	67
5	152	37	141	79
7	101	50	75	77

7	88	50	75	80
2	5	130	79	69
5	115	37	141	78
11	23	124	117	83
5	123	37	141	65

   Así que el mensaje en números es: 69 83 84 79 69 83 85 78 65 82 69 67 79 77 80 69 78 83 65

   Transformándolo a letras: ESTOESUNARECOMPENSA

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

   Para calcular el símbolo de Jacobi se usó ayuda del siguiente algoritmo (Schneier p. 252):

```
def jacobi(a,n):
    if n%2 == 0:
        return 2

    if a >= n:
        a = a%n
    if a == 0:
        return 0
    if a == 1:
        return 1

    if a<0:
```

```
        if ((n-1) // 2) % 2 == 0:
            return jacobi(-a,n)
        else:
            return -jacobi(a,n)

    if a%2 == 0:
        if ((n*n-1) // 8) % 2 == 0:
            return jacobi(a//2,n)
        else:
            return -jacobi(a//2,n)

    g = mcd(a,n)
    if a == g:
        return 0
    elif g != 1:
        return jacobi(g,n)*jacobi(a//g,n)
    elif (((a-1)*(n-1))//4) % 2 == 0:
        return jacobi(n,a)
    else:
        return -jacobi(n,a)
```

Pasos para comprobar si n es primo.

Se elige un número aleatorio a menor que n: 2343. Se calcula el máximo común divisor de 2343 de 23999, que es 1. Se calcula $j = a^{(p-1)/2} \mod p$; esto es $2343^{11999} \mod 23999 = 4244$. Se calcula el símbolo de Jacobi: $J(2343, 23999) = -1$. Como $4244 \neq -1$, es decir $j \neq J(a, n)$ se tiene que el número no es primo.

5. Descomponer a n=2399 con el algoritmo de rho de pollard.
   Para resolver el problema nos resultó más facil programar el algoritmo de rho de pollard en python:

```
def pollard(k,n):
    if k == 0:
        return 2
    return (( pollard(k-1,n)**2 ) + 1)%n

def mcd(a, b):
        resto = 0
        while(b > 0):
                resto = b
                b = a % b
                a = resto
        return a

def ejecuta_pollard(n,iteraciones):
    for i in range(iteraciones):
        a = pollard(i, n)
        b = pollard(i*2, n)
        resta = a-b
        print (i,a,b,resta,mcd(resta,n),"\n")

ejecuta_pollard(23999, 13)
```

En la función *pollard* es en donde se implementa el algoritmo de manera recursiva y simplemente se manda a llamar en el for para descubrir cuándo el mcm es diferente de 1 y n, ejecutando el programa con 20 iteraciones, en **i=12**, se tiene que **mcd=233**, y este es el divisor primo más grande de n, y el más chico es **103**, por lo que **233*103=23999**. la siguente es la tabla con los datos de la salida del programa:

i	x_i	x_{2i}	$x_i - x_{2i}$	mcd($x_i - x_{2i}, n$)
1	5	26	-21	1
2	26	2349	-2323	1
3	677	9186	-8509	1
4	2349	956	1393	1
5	22031	12788	9243	1
6	9186	18670	-9484	1
7	2113	4923	-2810	1
8	956	3991	-3035	1
9	1975	14709	-12734	1
10	12788	12379	409	1
11	3759	14243	-10484	1
12	18670	7020	11650	233

6. Descomponer a n=2399 con el algoritmo de rho-1 de pollard.

   a) Escogemos como cota de homogeneidad 37

   b) Tomamos un entero a menor que n, tal que $mcd(a, n) = 1$, entonces tomamos $a = 2$

   c) Calculamos la tabla para los valores de q que es un primo $q \leq \beta$, l y a', sabiendo que:

$$l = \left\lfloor \frac{ln(n)}{ln(q)} \right\rfloor$$

$$a' = a^{q^l} mod(n)$$

q	l	a	mcd(a-1,n)
2	14	6641	1
3	9	15320	1
5	6	2565	1
7	5	10083	1
11	4	2711	1
13	3	17334	1
17	3	11022	103

   d) Como ya se encontró un número que no fuera primo relativo con n, en la última fila de la tabla, no se tuvo que seguir calculando los demás, y por lo tanto un divisor no trivial de 23999 es 103, y finalmente **103*233=23999**

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

   a)

$$x^2 \cong 23999 \quad \text{mód } (2)$$

$$\Rightarrow x^2 \cong 1 \quad \text{mód } (2)$$

$$\Rightarrow x = 1$$

b)

$$x^2 \cong 23999 \quad \text{mód } (5)$$
$$\Rightarrow x^2 \cong 4 \quad \text{mód } (5)$$
$$\Rightarrow x = 2$$

c)

$$x^2 \cong 23999 \quad \text{mód } (13)$$
$$\Rightarrow x^2 \cong 1 \quad \text{mód } (13)$$
$$\Rightarrow x = 1$$

d)

$$x^2 \cong 23999 \quad \text{mód } (73)$$
$$\Rightarrow x^2 \cong 55 \quad \text{mód } (73)$$
$$\Rightarrow x = 36$$
$$36 * 36 \cong 1296 \cong 55 \quad \text{mód } 73$$

Por lo que para 2, 5, 13 y 73, 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 qué sirve cada una.

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

   c) dar 157^{-1} mód $(\phi(n))$

$$157 * x \cong 1 \quad \text{mód } (phi(n))$$
$$\Rightarrow 157 * x \cong 1 \quad \text{mód } ((233-1)(103-1))$$
$$\Rightarrow 157 * x \cong 1 \quad \text{mód } (23664)$$
$$\Rightarrow x = 12661 = 157^{-1}$$

   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.

M', 'U', 'C', 'H', 'A', 'C', 'H', 'O', 'S', 'Q', 'U', 'E', 'T', 'E', 'N', 'G', 'A', 'N', 'U', 'N', 'A', 'F', 'E', 'L', 'I', 'Z', 'N', 'A', 'V', 'I', 'D', 'A', 'D', 'Y', 'F', 'E', 'L', 'I', 'C', 'E', 'S', 'V', 'A', 'C', 'A', 'C', 'I', 'O', 'N', 'E', 'S', 'E', 'N', 'C', 'O', 'M', 'P', 'A', 'N', 'I', 'A', 'D', 'E', 'S', 'U', 'S', 'S', 'E', 'R', 'E', 'S', 'Q', 'U', 'E', 'R', 'I', 'D', 'O', 'S', 'L', 'E', 'S', 'A', 'P', 'R', 'E', 'C', 'I', 'A', 'M', 'O', 'S', 'S', 'U', 'S', 'P', 'R', 'O', 'F', 'E', 'S', 'O', 'R', 'E', 'S'