Universidad Nacional Autónoma de México
Facultad de Ciencias
Criptografía y Seguridad

Tarea 3
Curvas elípticas

Ángel Iván Gladín García
No. cuenta: 313112470
angelgladin@ciencias.unam.mx

Melanie Bautista Cruz
No. cuenta: 313181711
mbautista@ciencias.unam.mx

24 de Mayo 2019

1. Sea la curva elíptica $E := 0 = y^2 - x^3 - x - 9$ definida sobre $\mathbb{Z}_{17}$

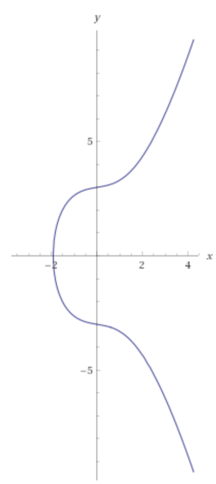

Figura 1: Curva elíptica de la forma $y^2 = x^3 + x + 9$

(I) Calcule y muestre todos los puntos de E.
<u>**Solución:**</u> Por definición se consideran los puntos con coordenadas en algún campo $L \supseteq K$ que se escribirá como $E(L)$, por definición, este conjunto siempre contiene al punto ∞.

$$E(L) = \{\infty\} \cup \{(x, y) \in L \times L \mid y^2 = x^3 + Ax + B\}$$

Para encontrar los puntos de E, se procederá por calcular todos los puntos en la curva dejando correr los valores de $x \in [0, 16]$ y resolver para y. Sutituyendo cada uno de esos puntos y encontrar el valor y que resuelva la ecuación. Para hacerlo se hizo un programa en *Python*.

```
def encontrar_puntos(A, B, p):
    '''Función que encuentra los puntos de la curva tal que
    satisface la ecuación.
```

```
    Ecuación de la curva elíptica de Weierstrass
        y^2 = x^3 + Ax + B

    Arguments:
        A {[int]} -- [Constamte de la ecuación]
        B {[int]} -- [Constamte de la ecuación]
        p {[int]} -- [Primo del campo Z_p]
    '''

    # Lista que tendrá los puntos
    puntos = []

    # Iterar sobre los valores que tomará la x
    for i in range(p):
        # Calcular x^3 + Ax + B módulo p
        l = (pow(i, 3, p) + (A * i) + B) % p
        # Iterar sobre los valores que tomará la y
        for j in range(p):
            y_2 = pow(j, 2, p)
            # Verificar si satisface la congruencia
            if (y_2 - l) % p == 0:
                # Agregar el punto
                puntos.append((i, j,))

    return puntos

print(encontrar_puntos(A=1, B=9, p=17))
```

Con el programa previo se puede concluir que $|E| = 25$ y que los puntos son:

$$\{\mathcal{O}\} \cup \{(0,3),(0,14),(2,6),(2,11),(4,3),(4,14),(7,6),(7,11),(8,6),$$

$$(8,11),(9,4),(9,13),(10,4),(10,13),(11,5),(11,12),(12,7),(12,10),(13,3),$$

$$(13,14),(14,8),(14,9),(15,4),(15,13)\}$$

(II) Alicia desea enviar el siguiente mensaje $C = (a,b) = ((12,7),(11,12))$ a Bob, los parámetros públicos de Bob son $\alpha = (0,3) \in E$ una raíz primitiva y $\beta = (13,3)$, donde $\beta = s\alpha$ y s su llave privada. Usa cualquier algoritmo mencionado en la sección 5.2 del libro **Elliptic Curves Number Theory and Cryptography de Lawrence C. Washington** Para resolver el PLD.

Solución: Se uso estos scripts[1]. Siguiendo el algoritmo[2], α la raíz primitiva existe una k la que $M_1 = k\alpha$ que esto es $M_1 = (12,7) = k(0,3)$ teniendo que essto el la primera entrada de C. Para encontrar la k de M_2 (que es la segunda entrada de C) que es $(11,12) = M_2 = M + kB = M + k(13,3)$.
Tomando $m \geq \sqrt{5}$ calculando $n(0,3)$ con $n \in [0,4]$. Encontrando los inversos en $\mathbb{Z}_{17}^*$ y como

[1] `https://github.com/ashutosh1206/Crypton/tree/master/Elliptic-Curves` para la manipulación y operaciones sobre curvas elípticas.

[2] Página 146

$0(0,3) = (0,3) - (0,3)0$, $1(0,3) = (0,3)$ y $2(0,3) = (0,3) + (0,3)$.
Entonces $3(0,3) = (0,3) + (9,4)$. con $k = 3$ y $3(0,3) = (12,7)$.
Calculando $kB = k(13,3)$ entonces $kB = 3B = (7,11)$, entonces $M = (11,12) - (7,11)$ quedando así $M = (14,9)$.

(III) A partir de la información encontrada en (ii) descifra el mensaje enviado a Bob.
Solución: Usando ElGamal[3] siguiendo la fórmula de:

$$M = M_2 - sM_1$$

Se tiene que $M = (11,12) - s(12,7) = (11,12) - 7(12,7) = (11,2) - (7,11) = (11,12) + (7,6) = (14,9)$. Donde el mensaje original es $M = (14,9)$.

2. Sea $E := y^2 + 20x = x^3 + 21 \mod 35$ y sea $P = (15,-4) \in E$.

(I) Factoriza 35 tratando de calcular $3P$.
Solución: Sea E la curva elíptica $y^2 = x^3 - 20x + 21 \mod 35$ y sea $P = (15,-4)$. Primero se procedera a calcular la línea tangente pendiente del punto P. Dado que solo se tiene un punto, se usará la siguiente fórmula[4]:

$$m = \frac{dy}{dx} = \frac{3x_1^2 + A}{2y_1}$$

Entonces para encontrar m del punto P se aplicará la fórmula previa

$$m = \frac{3x_1^2 + A}{2y_1} = \frac{3(15)^2 - (20)}{2(-4)} = -\frac{25}{8} \mod 35$$

Se obtendrá el máximo común divisor del denominador de m y el módulo p, $gcd(8,35) = 1$. Dado que es 1, se calculará[5] el inverso módulo p del denominador de la pendiente m, el cual es, $8^{-1} \equiv 22 \mod 35$.
Teniendo el inverso, la pendiente queda como:

$$-\frac{25}{8} \cdot (8^{-1}) = -\frac{25}{8} \cdot (22) \equiv 10 \mod 35$$

Para encontrar $2P$, teniendo solamente P y utilizando su pendiente utilizaremos la siguiente fórmula[6]:

Si $P_1 = P_2 \quad \wedge \quad y_1 \neq 0 \quad$ entonces $\quad x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad$ donde $m = \dfrac{3x_1^2 + A}{2y_1}$

Sustituyendo en la fórmula previa para calcular $2P = (x,y)$ con $m = 10$ se tiene

$$x \equiv (10)^2 - 2(15) \equiv 0, \qquad y \equiv (10)((15) - (0)) - (-4) \equiv 14$$

[3] Página 175
[4] Se explica bien el porqué en la página 13 de la bibliografía.
[5] Use esta herrmienta para calcular inversos multiplicativos módulo p, `https://planetcalc.com/3311/`
[6] Para más detalles ver página 14, ahí explica los posibles casos para calcular puntos.

Con $2P = (0, 14)$.

Para calcular $3P$, sumamos bajo la operación del grupo a P y $2P$, con la siguiente fómula[7]:

$$\text{Si } x_1 \neq x_2, \text{ entonces } x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{ donde } m = \frac{y_2 - y_1}{x_2 - x_1}$$

Teniendo así que la pendiente m es:

$$\frac{14 - (-4)}{0 - 15} = -\frac{19}{15}$$

Tomando el denominador del m previo y el primo p, entonces $gcd(15, 35) = 5 \neq 1$. Por consiguiente, no se puede encontrar $15^{-1} \mod 35$ y no se puede evaluar la tangente.
Ergo se ha encontrado un factor de 35 que es 5 quedando así la descomposición requerida

$$35 = 5 \cdot 7$$

(II) Factoriza 35 tratando de calcular $4P$ duplicándolo.
<u>**Solución:**</u> Teniendo previamente calculado $2P = (0, 14)$, se puede ver[8] a $4P$ como $4P = 2P + 2P$ usando la operación definida en el grupo con la siguiente condición:

$$\text{Si } P_1 = P_2 \quad \wedge \quad y_1 \neq 0 \quad \text{ entonces } m = \frac{3x_1^2 + A}{2y_1}$$

Calculando la pendiente de $4P$ queda:

$$m = \frac{3(0)^2 + (-20)}{2(14)} = -\frac{20}{28} \mod 35$$

Como $gcd(35, 28) = 7 \neq 1$. Por tanto tratando de calcular $4P$ se obtuvo que 7 es un factor de 35 quedando así:

$$35 = 7 \cdot 5$$

(III) Calcula ambos $3P$ y $4P$ sobre $E \mod 5$ y sobre $E \mod 7$ explica por que el factor 5 se obtiene calculando $3P$ y el factor 7 se obtiene calculando $4P$.
<u>**Solución:**</u>

Usando el código descrito en el ejercicio (4a), obtenemos que

- 3P mod 5 = (0,0)
- 4P mod 5 = (0,1)
- 3P mod 7 = (1,4)
- 4P mod 7 = (0,0)

Por lo que para $3P$ obtuvimos ínf $mod 5$ y un punto finito $mod 7$, por esta razón la pendiente tenía un 5 en el denominador y por lo tanto fue infinito módulo 5. Por otro lado el orden de $P mod 7$ es 4, si su orden hubiera sido *3* la pendiente habría tenido un $0 mod 35$ en su denominador y su mcd habría sido 35, lo que indicaría que no se obtuvo la factorizción de 35. En este ejercicio esta comprobación no es necesaria, pero para números primos mucho más grandes, es un paso necesario.

[7] Página 14 en la sección de *GROUP LAW*, propiedad 1.
[8] Página 14 en la sección de *GROUP LAW*, propiedad 3.

3. Alicia quiere firmar un mensaje utilizando el esquema ElGamal elíptico con los siguientes parámetros: $p = 314159$, $a = 217$, $b = 2006$, $P = (123456, 43989)$, $n = 314423$. Su clave privada es $d = 223344$ y su clave pública es $Q = (216438, 187612)$.

(I) Si el mensaje que quiere firmar es $m = 6500$ (cantidad de pesos que quiere retirar de su cuenta mediante una transferencia bancaria), ¿cuál es la firma digital de m? (supongamos que el entero aleatorio k tal que $1 \leq k \leq n-1$ que se tiene que escoger es igual a 666).
<u>**Solución:**</u> Sea m que representa al documento, un entero k tomado aleatorio, tomando $k = 666$ y N tal que $gcd(k, N) = gcd(666, 314423) = 1$. Se calculará $R = kA$ donde $R = 666(123456, 43989)$ y evaluando el producto del punto por un escalar se tiene que $R = (2939{,}140788) = 666P$.
Sieguienedo el úlitmo paso del algoritmo[9] se tiene que calcular

$$s \equiv k{-}1(m - af(R)) \mod N$$

que esto eso $s = (666)^{-1} * (6500 - 217f(R)) \mod 314432$.
Qudando así las firma digital como la tripleta $(m, R, s) = (6500, (2939, 140788), 205065)$.

(II) ¿Qué cómputos tiene que hacer el banco para verificar la firma de Alicia?
<u>**Solución:**</u> Para que el banco verifique que la llave de Alicia de tienen que hacer los siguientes pasos:

- Descargar la información pública de Alicia

$$(6500, (2939, 140788), 205065)$$

- Calcular $V_1 = f(R)B + sR$ y $V_2 = mA$.
  Calculando $V_1 = (203478, 24120) + (99360, 230917) = (283710, 77429)$.
  Calculando $V_2 = 6500 = (283710, 77429)$
- Si $V_1 = V_2$ entonces la firma es válida:
  Como $V_1 = V_2$ entonces la firma es válida.

4. Sea $\mathbf{E} : y^2 = x^3 + 333x + 2$ sobre $\mathbb{F}_{347}$ y sea $P = (110, 136)$

a) Si sabemos que $|\mathbf{E}| = 358$ ¿Podemos decir que $\mathbf{E}$ es criptográficamente útil?, ¿Cuál es el orden de P? ¿Entre que valores se puede escoger la clave privada? <u>**Solución:**</u>

Sabemos que los puntos de la curva elíptica $y^2 = x^3 + ax + b$ definen un grupo abeliano en $\mathbf{F}_q$ si

$$(4a^3 + 27b^2) mod p \neq 0 mod p \tag{1}$$

En este caso $4 * 33^3 + 27 * 2^2 = 236 mod 347$ Por lo que la curva puede ser usada para encriptar. Como $|\mathbf{E}| = 358 = 179 * 2$, en la práctica no sería usada pues su tamaño es muy pequeño.

El orden de P, que es el entero positivo k más pequeño tal que $kP = \infty$, calculamos k de la forma descrita en la sección 4.3.3 del libro **Elliptic Curves, Number Theory and**

[9] Pagína 176, paso 3

Cryptography, Lawrence C. Washington, usando el algoritmo de *Paso grande, paso chico*

Las siguientes son algunas funciones generales, programadas en Julia (plataforma en línea https://juliabox.com)

```
# Funci n que calcula el inverso de un n mero en Zp
function inverso_unidad(a, mod)
    u0, u1 = 1, 0
    v0, v1 = 0, 1

    while mod != 0
        q = floor(a/mod)
        r = a - mod * q
        u = u0 - q * u1
        v = v0 - q * v1
        #Update a,b
        a = mod
        mod = r
        #Update for next iteration
        u0 = u1
        u1 = u
        v0 = v1
        v1 = v
    end

    return  a, u0, v0
end

#Funcion que verifica que una congruencia tenga solucion
function cong_val(a,b,n)
    j = gcd(a,n)
    ans = false
    if b %j == 0
        ans = true
    end

    return ans
end

# solve_congruencia(a, b, n) soluciona la congruencia usando el algoritmo extendido de Euclides.
function congruencias(a,b,n)
    if cong_val(a,b,n)
        # Reduciendo la congruencia
        m_c_d = gcd(a,n)
        a, n, b = a/m_c_d, n/m_c_d, b/m_c_d

        a_inverso = (inverso_unidad(a, n)[2] + n) %n

        x = (b * a_inverso) %n
        #x = x * m_c_d
    else
        x = "La congruencia no es v lida"
    end

    return x
end
```

```
#Funci n que suma dos puntos diferentes P,Q en una curva el ptica
function pnt_add(P, Q, mod)

    lam = ((Q[2] - P[2]) %mod)//(Q[1] - P[1])
    if denominator( ) != 1
        lam = congruencias(denominator(lam), numerator(lam), mod)
        else
        lam = numerator(lam)
    end
    lam = (mod + lam) %mod
    x = (lam^2 - P[1] - Q[1]) %mod
    y = (lam*(P[1]-x) - P[2]) %mod
    x = (mod + x) %mod
    y = (mod + y) %mod

    return [Int(x),Int(y)]

end

#Funcion que calcula P+P= 2P en una curva eliptica
function pnt_double(P, a, mod)
    Q = P
    lam = ((3*P[1]^2 + a) %mod)//(2*P[2])
    if denominator(lam) != 1
        lam = congruencias(denominator(lam), numerator(lam), mod)
        else
        lam = numerator(lam) %mod
    end
    lam = (mod + lam) %mod
    x = (lam^2 - P[1] - Q[1]) %mod
    y = (lam*(P[1]-x) - P[2]) %mod
    x = (mod + x) %mod
    y = (mod + y) %mod

    return [Int(x),Int(y)]

end

#Funcion que regresa la representacion binaria de un n mero decimal
function binary_s(d)

    a = bitstring(d)
    if d != 0
        l = "1"*split(a,'1'; limit=2)[2]
        else
        l = "0"
    end
    return l
end

# Funcion que multiplica a un numero por un escalar d, representado en la forma binaria $d = d_{0} + 2^{w}d_{1} + 2^{2w}d_{2} + ... + 2^{mw}d_{m}$
function pnt_k(P, d, a, mod)
    N = P
    Q = [0,0]
    l = binary_s(d)
    m = length(l)

    for i in m:-1:1
```

```
        if l[i] == '1'
            if Q[1] != 0 || Q[2] != 0
                Q = pnt_add(N, Q, mod)
            else
                Q = N
            end
        end
        N = pnt_double(N, a, mod)
    end

    return Q
end
```

El algoritmo de *Paso grande, paso chico* para el punto P, es el siguiente

a) Calcula Q = (q+1)P

b) Elige un entero m tal que $m > q^{1/4}$. Calcula y guarda los puntos jP para j = 0, 1, 2,...,m

```
m = Int(ceil(q^(1/4)))
Js = [[0,0] for i in 0:2m+1]

for i in 0:2:2*m
    Js[i+1] = pnt_k(P, Int(i/2), E[1], q)
    Js[i+2] = [Js[i+1][1], -Js[i+1][2]]
end
```

c) Calcula los puntos $Q+k(2mP)$ para $k = m, (m1), ..., m$ hasta que encuentres la igualdad $Q + k(2mP) = \pm jP$ Para algún punto (o su negativo) de la lista

```
p1 = pnt_k(P, 2*m, E[1], q)
k = 0
r = [0,0]

prueba = false
while prueba == false && k < m
    p2 = pnt_k(p1, k, E[1], q)
    r = pnt_add(Q, p2, q)
    prueba = (r in Js)
    k = k + 1

end
if k!=m  #Puede que haya un caso en el que k s   deba ser m, pero son raros
    k = k-1
end

j = 0
alph = Int((q +1 +2*m*k - j))
P2 = pnt_k(P, alph, E[1], q)
```

Con este resultado, concluimos que $(q + 1 + 2mk \mp j)P = \infty$

d) Sea $M = q + 1 + 2mk \mp j$, factoriza M, donde $p_1, ..., p_r$ sus factores primos. Calcula $(M/p_i)P$ para cada $i = 1, ..., r$. Si $(M/p_i)P =$ ínf entonces reemplaza M por M/p_i y vuelve a factoriza esta nueva M. Repite el proceso hasta que $(M/p_i)P \neq$ ínf para todo i. Entonces M es el orden de P.

```
using Primes

factrs = factor(Vector,  )
```

```
alph2 = Int(358/2)
P2 = pnt_k(P, alph2, E[1], q)

alph3 = Int(358/179)
P2 = pnt_k(P, alph3, E[1], q)
```

En nuestro caso $M = 2 * 179$, como $(M/2)P = \text{ínf}$ y $(M/179)P \neq \text{ínf}$, concluimos que 179 es el orden de P.

Los valores entre los que se puede escoger la llave privada están limitados por el orden de P = 179, por lo que $d \in [1, 179 - 1]$

b) Si tu clave privada es d = 101 y alg un conocido te ha enviado el mensaje cifrado (C1 = (232, 278), C2 = (135, 214)) ¿Cuál era el mensaje original?
Solución: En este cso, tenemos como sistema de encriptación a ElGamal. Para desencriptar, lo que debemos de hacer es calcular $M = C_2 - dM_1$, con d=101 la llave prvada. Para hacerlo es muy sencillo, usando las funciones anteriormente definidas, sólo calculamos lo siguiente

```
M1 = [232, 278]
M2 = [135, 214]
sM1 = pnt_k(M1, d, E[1], q)
m_sM1 = [sM1[1], -sM1[2]]

pnt_add([135,214],[275,-176],347)
```

Obteniendo como punto original a $M = (74, 87)$, y el mensaje original es m=74, debido a la forma en que se encripta un mensaje en ElGamal. Si quisieramos encontrar el número aleatorio k con el que fue cifrado el mensaje enviado, sólo debemos seguir el algoritmo de *paso grande, paso chico*

```
m = Int(ceil(sqrt(358)))
mP = pnt_k(P, m, E[1], q)

iP_s = [pnt_k(P, i, E[1], q) for i in 0:m-1]

j = 0
jmP = pnt_k(mP, j, E[1], q)
m_jmP = [Int(jmP[1]), -Int(jmP[2])]
res = pnt_add(Q,m_jmP,q)
res in iP_s
# Observamos que j = 0 se encuentra en iP_s, en el  ndice  i = 7
i = 7
k = (i + j*m)%q

# Corroboramos que kP = C1
pnt_k(P, k, E[1], q) == Q

#Calculamos M + kB y corroboramos que sea igual al C2 proporcionado
kB = pnt_k(B, k, E[1], q)
test_M2 = pnt_add(M, kB, q)
```

De esto obtenemos que $k = 7$, y comporbamos que el mensaje descifrado sí es correcto.

5. Sea $\mathbf{E}: y^2 = x^3 + 2x + 7$ sobre $\mathbb{Z}_{31}^*$ con $\#\mathbf{E} = 39$ y $P = (2, 9)$ es un punto de orden 39 sobre E, el ECIES simplicado definido sobre E tiene $\mathbb{Z}_{31}^*$ como espacio de texto plano, supongamos que la clave privada es $m = 8$

a) Calcula Q = mP
<u>Solución</u>: Usando las mismas funciones que en el ejercicio (4), obtenemos de forma inmediata que Q= (8,15)

b) Descifra la siguiente cadena de texto cifrado ((18, 1), 21),((3, 1), 18)),((17, 0), 19),((28, 0), 8) **<u>Solución</u>:** Sabemos que en el criptosistem ECIES simplificado, el mensaje cifrado es de la forma $((\mathbf{Z_p} \times \mathbf{Z_2}) \times \mathbf{Z}_p*) = (y_1, y_2)$.

Como el orden de $P = (2, 9)$ es el mismo que **E**, P es un generador y puede ser usado en la encriptación de ECIES simplificado.

Los puntos de compresión recibidos son: (18,1), (3,1), (17,0), (28,0) Debemos calcular sus respectivos puntos de descompresión. Sabemos que

$$z \leftarrow (x^3 + 2x + 7) mod 31 \tag{2}$$

Como z no es R-C mod 31, podemos evaluar

$$z \leftarrow y^2 = ((18)^3 + 2(18) + 7) mod 31 = 16 mod 31 \tag{3}$$

Por lo que $z = \pm 4 mod 31$ Sabemos que por construcción del punto de compresión, la segunda entrada se calcula al sacar $mod 2$ al punto kP, por lo que el valor de $z mod 2$ debe ser igual a la segunda entrada del punto de compresión, que en este caso es 1, de esta forma $z = -4 = 27 mod 31 = 1 mod 2$, cosa que no sucede con $z = 2 = 2 mod 31 = 0 mod 2$.

Como $Q = (8, 15)$, obtenemos el punto $8 * (18, 27) = (15, 8) = (x_0, y_0)$ Finalmente desciframos el mensaje, usando $d_k(y) = y_2 * (x_0)^{-1} mod q$, que en nuestro caso es

$$d_k = 21 * (15)^{-1} = 21 * 29 mod 31 = 20 mod 31 \tag{4}$$

Así que la primer letra de texto plano es $x_1 = 20$

Repetimos este procedimiento para el resto de los puntos de compresión:

- ((3,1), 18) $3^3 + 2 * 3 + 7 = 9 mod 31$ Por lo que $z = \pm 3$, y al ser el punto de compresión (3,**1**), entonces $z = 3 mod 31 = 1 mod 2$ Entonces $8 * (3, 3) = (2, 9)$, por lo que

$$d_k = 18 * (2)^{-1} = 18 * 16 mod 31 = 9 mod 31 \tag{5}$$

  Así que $x_2 = 9$

- ((17,0), 19) $17^3 + 2 * 17 + 7 = 25 mod 31$ Por lo que $z = \pm 5$, y al ser el punto de compresión (17,**0**), entonces $z = -5 mod 31 = 26 mod 31 = 0 mod 2$ Entonces $8 * (17, 26) = (30, 29)$, por lo que

$$d_k = 19 * (30)^{-1} = 19 * 30 mod 31 = 12 mod 31 \tag{6}$$

  Así que $x_3 = 12$

- ((28,0), 8) $28^3 + 2 * 28 + 7 = 5 mod 31$ Para encontrar la raíz de y, es más fácil si notamos que $5 mod 31 = 36 mod 31$ Por lo que $z = \pm 6$, y al ser el punto de compresión (20,**0**), entonces $z = 6 mod 31 = 0 mod 2$ Entonces $8 * (28, 6) = (14, 19)$, por lo que

  $$d_k = 8 * (14)^{-1} = 18 * 20 mod 31 = 5 mod 31 \tag{7}$$

  Así que $x_2 = 5$

Por lo tanto tenemos la cadena de texto plano $X = 20, 9, 12, 5$

c) Supongamos que cada texto plano representa un caracter alfab etico, convierte el texto plano en una palabra en ingles. usa la asociaci on (A → 1,. . . , Z → 26) en este caso 0 no es considerado como un texto plano o un par ordenado.

Solución: Notemos que no consideramos a la $\tilde{N}$ como parte del alfabeto, por lo que la cadena $(20, 9, 12, 5)$ tiene como equivalencia (T, I, L, E)

Referencias

[1] Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. 1996. *Handbook of Applied Cryptography (1st ed.).* CRC Press, Inc., Boca Raton, FL, USA.