# Facultad de Ciencias, UNAM
# Criptografía y Seguridad
# Tarea 3

Altamirano Vázquez Jesús Fernando
Rubí Rojas Tania Michelle

15 de septiembre de 2020

1. Sea $\mathbb{E} : y^2 + 20x = x^3 + 21 \pmod{35}$ y sea $Q = (15, -4) \in \mathbb{E}$.

   *a*) Factoriza 35 tratando de calcular $3Q$.
   SOLUCIÓN: Recordemos la definición de suma de puntos:

$$P + Q = \begin{cases} \infty & \text{Si } x_1 = x_2 \text{ y } -y_1 = y_2 \\ (x_3, y_3) & x_3 = \lambda^2 - x_1 - x_2 \text{ y } y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

   Al igual que debemos recordar como calcular $\lambda$ :

$$\lambda = \begin{cases} 3x_1^2 + A \cdot (2y_1)^{-1} \pmod{p} & \text{si } P = Q \\ (y_1 - y_2) \cdot (x_1 - x_2)^{-1} \pmod{p} & \text{en otro caso} \end{cases}$$

   Además, tenemos que $\mathbb{E} : y^2 = x^3 - 20x + 21$. Primero, obtendremos $2Q$, para lo cual obtendremos primero el valor de $\lambda$. Como $Q = Q$, entonces

$$\begin{aligned} \lambda &= 3(15)^2 + (-20) \cdot 2(-4)^{-1} \pmod{35} \\ &= (3 \cdot 255) - 20 \cdot (-8)^{-1} \pmod{35} \\ &= 655 \cdot 13 \pmod{35} \\ &= 8515 \pmod{35} \\ &= 10 \end{aligned}$$

   Ahora, calculamos el valor de $x_3$:

$$\begin{aligned} x_3 &= 10^2 - 15 - 15 \pmod{35} \\ &= 100 - 30 \pmod{35} \\ &= 70 \pmod{35} \\ &= 0 \end{aligned}$$

   Finalmente, calculamos $y_3$:

$$\begin{aligned} x_3 &= 10(15 - 0) - (-4) \pmod{35} \\ &= 150 + 4 \pmod{35} \\ &= 154 \pmod{35} \\ &= 14 \end{aligned}$$

Por lo tanto, $2Q = (0, 14)$. Ahora bien, procedemos a calcular $3Q = 2Q + Q$, y para ello realizamos los mismos pasos que en el cálculo anterior: como $2Q \neq Q$ entonces

$$\begin{aligned}\lambda &= (14 - (-4)) \cdot (0 - 15)^{-1} \pmod{35} \\ &= 18 \cdot (-15)^{-1} \pmod{35}\end{aligned}$$

Pero, 15 no tiene inverso multiplicativo en este caso, por lo que debemos encontrar el máximo común divisor de $(35, 15)$, el cual es 5. De esta forma, determinamos que 5 es un factor de 35.

*b*) Factoriza 35 tratando de calcular $4Q$ duplicándolo.
SOLUCIÓN: Como ya tenemos calculado $2Q$, entonces haremos $2Q + 2Q$ para obtener $4Q$. Así,

$$\begin{aligned}\lambda &= 3(0)^2 + (-20) \cdot (2 \cdot 14)^{-1} \pmod{35} \\ &= -20 \cdot (28)^{-1}\end{aligned}$$

Pero, $28 = 2 \cdot 14$ no tiene inverso multiplicativo, por lo que debemos calcular el $MCD(28, 35)$, el cual es 7. De esta forma, podemos concluir que 7 es un factor de 35.

*c*) Calcula $3Q$ y $4Q$ sobre $\mathbb{E}$ (mód 5) y sobre $\mathbb{E}$ (mód 7). Explica por qué el factor 5 se obtiene calculando $3Q$ y por qué el factor 7 se obtiene calculando $4Q$.
SOLUCIÓN:

- $3Q$ sobre $\mathbb{E}$ (mód 5). Tenemos que

$$\begin{aligned}\mathbb{E} : y^2 &= x^3 - 20x + 21 \pmod{35} \\ &= x^3 + 1 \pmod{35}\end{aligned}$$

Ahora bien, primero calcularemos $2Q$. Como $Q = (15, -4) = (0, 1) = Q$, entonces

$$\begin{aligned}\lambda &= (3(0)^2 + 0) \cdot (2 \cdot 1)^{-1} \pmod{5} \\ &= 0 \cdot (2)^{-1} \pmod{5} \\ &= 0 \cdot 3 \pmod{5} \\ &= 0\end{aligned}$$

Luego, calculamos $x_3$:

$$x_3 = (0)^2 - 0 - 0 \pmod{5} = 0$$

Finalmente, calculamos $y_3$:

$$\begin{aligned}y_3 &= 0(0 - 0) - 1 \pmod{5} \\ &= 0 - 1 \pmod{5} \\ &= 4\end{aligned}$$

Por lo tanto, $2Q = (0, 4)$.
Para calcular $3Q$ haremos $2Q + Q$. Como los puntos son diferentes, entonces

$$\begin{aligned}\lambda &= (4 - 1) \cdot (0 - 0)^{-1} \pmod{5} \\ &= 5 \cdot 0 \pmod{5} \\ &= 0\end{aligned}$$

Como $MCD(5, 0) = 5$, entonces tenemos que 5 es un factor de 5.

- $4Q$ sobre $\mathbb{E}$ (mód 7). Tenemos que

$$\begin{aligned}\mathbb{E} : y^2 &= x^3 - 20x + 21 \pmod 7 \\ &= x^3 + x \pmod 7\end{aligned}$$

Ahora bien, primero calcularemos $2Q$. Como $Q = (15, -4) = (1, 3) = Q$ entonces

$$\begin{aligned}\lambda &= (3(1)^2 + 1) \cdot (2 \cdot 3)^{-1} \pmod 7 \\ &= (3 + 1) \cdot (6)^{-}1 \pmod 7 \\ &= 4 \cdot 6 \pmod 7 \\ &= 24 \pmod 7 \\ &= 3\end{aligned}$$

Calculamos $x_3$:

$$\begin{aligned}x_3 &= (3)^2 - 1 - 1 \pmod 7 \\ &= 9 - 2 \pmod 7 \\ &= 7 \pmod 7 \\ &= 0\end{aligned}$$

Calculamos $y_3$:

$$\begin{aligned}y_3 &= 3(1 - 0) - 3 \pmod 7 \\ &= 3 - 3 \pmod 7 \\ &= 0\end{aligned}$$

Por lo tanto, $2Q = (0, 0)$.
Ahora bien, para calcular $4Q$ haremos $2Q + 2Q$. Como los dos puntos son iguales, entonces

$$\begin{aligned}\lambda &= (3(0)^2 + 1) \cdot (2 \cdot 0)^{-1} \pmod 7 \\ &= 1 \cdot (0)^{-1} \pmod 7\end{aligned}$$

Pero 0 no tiene inverso multiplicativo en este caso, y como $MCD(7, 0) = 7$ entonces tenemos que 7 es un factor de 7.

En cada suma se verifica si el máximo común divisor de (5 o 7) y $k$ es diferente de 1 (donde $k$ es el número al cual le sacaremos el inverso en la lambda). Si el $MCD$ no es 1, eso significa que existe un entero $n$ que divide a 5 y a $k$, pero como 5 y 7 son primos, eso quiere decir que ellos mismos son los números que se dividen. Por este motivo, obtenemos a 5 y 7 como factores.

2. Sea $\mathbb{E}$ la curva elíptica $y^2 = x^3 + x + 28$ definida sobre $\mathbb{Z}_{71}$.

   *a*) Calcula y muestra el número de puntos de $\mathbb{E}$.
   Solución: Sabemos que los puntos en una curva elíptica

$$E : y^2 = x^3 + Ax + B \pmod n$$

son los pares $(x, y) \pmod n$ con $x, y \in K$ tales que satisfacen la ecuación anterior, junto con el punto en el infinito.
Dada la siguiente implementación

```
        '''
        Regresa los puntos que pertenecen a la curva eliptica
        E: y^2 = x^3 + Ax + B (mod n)
        '''
        def encontrar_puntos(A, B, n):
            puntos = []
            # Sabemos que x pertenece al conjunto [0, 70].
            for i in range (0, n):
                # Sabemos que y pertenece al conjunto [0, 70].
                for j in range (0, n):
                    # Encontramos el valor de x^3 + Ax + B (mod n)
                    valor = (pow(i, 3, n) + ((A * i) % n) + B) % n
                    # Encontramos los posibles valores para y.
                    y2 = pow(j, 2)
                    # Verificamos que el par satisface la ecuacion.
                    if (((y2 - valor) % n) == 0):
                        puntos.append((i, j))

            print("La curva eliptica E tiene " + str(len(puntos) + 1) +
                  " puntos.")
            return puntos

        if __name__ == "__main__":
            print(encontrar_puntos(1, 28, 71))
```

obtenemos que, junto con el punto en el infinito, hay 72 puntos en la curva elíptica, los cuales son:

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| (1, 32) | (1, 39) | (2, 31) | (2, 40) | (3, 22) | (3, 49) | (4, 5) | (4, 66) | (5, 4) |
| (5, 67) | (6, 26) | (6, 45) | (12, 8) | (12, 63) | (13, 26) | (13, 45) | (15, 9) | (15, 62) |
| (19, 27) | (19, 44) | (20, 5) | (20, 66) | (21, 3) | (21, 68) | (22, 30) | (22, 41) | (23, 19) |
| (23, 52) | (25, 22) | (25, 49) | (27, 0) | (31, 32) | (31, 39) | (33, 1) | (33, 70) | (34, 23) |
| (34, 48) | (35, 14) | (35, 57) | (36, 12) | (36, 59) | (37, 33) | (37, 38) | (39, 32) | (39, 39) |
| (41, 7) | (41, 64) | (43, 22) | (43, 49) | (47, 5) | (47, 66) | (48, 11) | (48, 60) | (49, 24) |
| (49, 47) | (52, 26) | (52, 45) | (53, 0) | (58, 27) | (58, 44) | (61, 15) | (61, 56) | (62, 0) |
| (63, 17) | (63, 54) | (65, 27) | (65, 44) | (66, 18) | (66, 53) | (69, 35) | (69, 36) | $\infty$ |

*b*) Muestra que $\mathbb{E}$ no es un grupo cíclico.

*Demostración.* Sabemos que un elemento $P \in E$ es un punto primitivo si genera a todo el conjunto de puntos que pertenecen a $E$, es decir, todos los elementos del grupo pueden ser expresados de la forma

$$P + P + \cdots + P(k \text{ veces}) \quad \text{para alguna } k \in \{1, 2, ..., \#E(\mathbb{F}_q)\}$$

Por un corolario del teorema de *Lagrange* sabemos que el órden de un subgrupo generado por un elemento en $E$ necesariamente divide a $\#E(\mathbb{F}_q) = 72$, por lo que

$$D = \{1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36\}$$

son los posibles valores para el órden de cada uno de los puntos en $E(\mathbb{F}_{71})$, ya que son justamente todos los divisores de 72.

Por el ejercicio *2.c* sabemos que el órden de cada uno de los elementos en $E$ se encuentra dentro del conjunto

$$O = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

Entonces, como

$$\#E(\mathbb{F}_{71}) = n = 72 = 2^3 \cdot 3^2$$

no es primo, podemos buscar al punto primitivo $P$ de la siguiente forma: para cada primo $p$ que divide a 72, calculamos $(\frac{n}{p})P$. Si ninguno de estos puntos es el punto en el infinito, entonces $P$ genera a $E$. Por ejemplo, si $P = (1, 32)$ tenemos que

$$\left(\frac{72}{2}\right) P = 36(1, 32) = \infty$$
$$\left(\frac{72}{3}\right) P = 24(1, 32) = (20, 5)$$

Como $36P = \infty$, entonces no genera a $E$.

Ahora bien, podemos seguir el siguiente camino: el órden de un elemento en $E$ siempre será múltiplo de 36 o 24, y eso implica que $kP$, con $k = |P| \cdot i = 36$ *o* 24, genera el punto en el infinito. Tomando un elemento $P$ cuyo órden pertenezca al conjunto $O$, tenemos que

$$|P = (1, 32)| = 18 \Rightarrow 18 \cdot 2 = 36 \Rightarrow 36P = \infty$$
$$|P = (2, 31)| = 6 \Rightarrow 6 \cdot 4 = 24 \Rightarrow 24P = \infty$$
$$|P = (3, 22)| = 12 \Rightarrow 12 \cdot 2 = 24 \Rightarrow 24P = \infty$$
$$|P = (4, 5)| = 36 \Rightarrow 36 \cdot 1 = 36 \Rightarrow 36P = \infty$$
$$|P = (5, 4)| = 4 \Rightarrow 4 \cdot 6 = 24 \Rightarrow 24P = \infty$$
$$|P = (20, 5)| = 3 \Rightarrow 3 \cdot 8 = 24 \Rightarrow 24P = \infty$$
$$|P = (27, 0)| = 2 \Rightarrow 2 \cdot 12 = 24 \Rightarrow 24P = \infty$$
$$|P = (31, 32) = 9 \Rightarrow 9 \cdot 4 = 36 \Rightarrow 36P = \infty$$

Notemos que todas las operaciones fueron verificadas con la función `suma_puntos()`, implementada en el ejercicio *2.c*.

Como $|\infty| = 1$ no puede ser el generador del grupo, y el órden del resto de los puntos en $E$ oscila entre los valores del conjunto $O$, eso quiere decir que todos los puntos generan el punto en el infinito, lo que implica que $E$ no es generado por ninguno de sus elementos. Por lo tanto, $E$ no es cíclico.

□

*c*) ¿Cuál es el máximo órden de un elemento en $\mathbb{E}$? Encuentra un elemento que tenga este órden.

Solución: Por un corolario del teorema de *Lagrange* sabemos que el órden de un punto siempre divide el órden del grupo $E(\mathbb{F}_{71})$.

Dada la siguiente implementación

```
        # Regresa los divisores de un numero n.
        def divisores(n):
            div = []
            for i in range (1, n):
                if ((n % i) == 0):
                    div.append(i)

            return div

        if __name__ == "__main__":
            print(divisores(72))

```

sabemos que

```
D = [1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36]
```

son los posibles valores para el órden de cada uno de los puntos en $E(\mathbb{F}_{71})$. En particular, por el teorema de *Lagrange* tenemos que $\#E(\mathbb{F}_{71})P = 72P = \infty$, con $P \in E(\mathbb{F}_{71})$.

Ahora bien, el órden de un punto en $E(\mathbb{F}_{71})$ será el mínimo entero $k \in D$ tal que $kP = \infty$.

Dada la siguiente implementación

```
        '''
        Regresa una tupla (mcd, s, t) que obtenemos al aplicar el algoritmo
        extendido de Euclides, donde as + bt = mcd(a, b) son los elementos
        que conforman la tupla.
        '''
        def aee(a, b):
            s = 0; s_i = 1
```

```
            t = 1; t_i = 0
            g = b; g_i = a

            while g != 0:
                cociente = g_i // g
                g_i, g = g, g_i - cociente * g
                s_i, s = s, s_i - cociente * s
                t_i, t = t, t_i - cociente * t
            return (g_i, s_i, t_i)

        # Regresa el inverso multiplicativo de a modulo m.
        def inverso(a, m):
            g, s, t = aee(a, m)
            # El inverso de a modulo m existe si y solo si (a, m) = 1.
            if g != 1:
                print("No tiene inverso multiplicativo.")
            else:
                inverso = s % m

            return inverso

        # Regresa la suma de dos puntos P y Q en E.
        def suma_puntos(P, Q, A, p):
            # Casos especiales.
            if (P == None):
                return Q
            if (Q == None):
                return  P

            x1, y1 = P
            x2, y2 = Q

            if (x1 == x2):
                m = (3 * x1 * x1 + A) * inverso(2 * y1, p)
            else:
                m = (y1 - y2) * inverso(x1 - x2, p)

            x3 = m * m - x1 - x2
            y3 = m * (x1 - x3) - y1
            suma = (x3 % p, y3 % p)
            return suma

        # Regresa el orden de un elemento en E.
        def orden(P, a, p):
            # Como P = P y y_1 = 0 entonces P+P = infinito.
            if(P[1] == 0):
                return 2

            # Calculamos 2P.
            P2 = suma_puntos(P, P, a, p)
            aux = P2

            orden = 3
            for i in range(0, p):
                # Calculamos P + kP
                aux = suma_puntos(P, aux, a, p)
                # Si encontramos a 2P, entonces hemos encontrado el orden.
                if(aux == P2):
                    break
                orden += 1
            return orden
```

```
69
70          # Regresa el orden de cada uno de los elementos en la lista puntos.
71          def get_ordenes(puntos, a, p):
72              ordenes = []
73              for punto in puntos:
74                  o = orden(punto, a, p)
75                  ordenes.append(o)
76
77              return ordenes
78
79          if __name__ == "__main__":
80              print(get_ordenes(encontrar_puntos(1, 28, 71), 1, 71))
81
```

obtenemos la siguiente tabla, la cual indica el órden de cada uno de los elementos que pertenecen a $E$.

| | | | | |
|---|---|---|---|---|
| $\|(1,32)\| = 18$ | $\|(1,39)\| = 18$ | $\|(2,31)\| = 6$ | $\|(2,40)\| = 6$ | $\|(3,22)\| = 12$ |
| $\|(3,49)\| = 12$ | $\|(4,5)\| = 36$ | $\|(4,66)\| = 36$ | $\|(5,4)\| = 4$ | $\|(5,67)\| = 4$ |
| $\|(6,26)\| = 18$ | $\|(6,45)\| = 18$ | $\|(12,8)\| = 18$ | $\|(12,63)\| = 18$ | $\|(13,26)\| = 36$ |
| $\|(13,45)\| = 36$ | $\|(15,9)\| = 36$ | $\|(15,62)\| = 36$ | $\|(19,27)\| = 6$ | $\|(19,44)\| = 6$ |
| $\|(20,5)\| = 3$ | $\|(20,66)\| = 3$ | $\|(21,3)\| = 36$ | $\|(21,68)\| = 36$ | $\|(22,30)\| = 18$ |
| $\|(22,41)\| = 18$ | $\|(23,19) = 36$ | $\|(23,52)\| = 36$ | $\|(25,22)\| = 18$ | $\|(25,49)\| = 18$ |
| $\|(27,0)\| = 2$ | $\|(31,32)\| = 9$ | $\|(31,39)\| = 9$ | $\|(33,1)) = 36$ | $\|(33,70)\| = 36$ |
| $\|(34,23)\| = 36$ | $\|(34,48)\| = 36$ | $\|(35,14)\| = 12$ | $\|(35,57)\| = 12$ | $\|(36,12)\| = 9$ |
| $\|(36,59)\| = 9$ | $\|(37,33)\| = 36$ | $\|(37,38)\| = 36$ | $\|(39,32)\| = 6$ | $\|(39,39)\| = 6$ |
| $\|(41,7)\| = 36$ | $\|(41,64)\| = 36$ | $\|(43,22)\| = 36$ | $\|(43,49)\| = 36$ | $\|(47,5)\| = 36$ |
| $\|(47,66)\| = 36$ | $\|(48,11)\| = 36$ | $\|(48,60)\| = 36$ | $\|(49,24)\| = 4$ | $\|(49,47)\| = 4$ |
| $\|(52,26)\| = 12$ | $\|(52,45)\| = 12$ | $\|(53,0)\| = 2$ | $\|(58,27)\| = 18$ | $\|(58,44)\| = 18$ |
| $\|(61,15)\| = 18$ | $\|(61,56)\| = 18$ | $\|(62,0)\| = 2$ | $\|(63,17)\| = 9$ | $\|(63,54)\| = 9$ |
| $\|(65,27)\| = 18$ | $\|(65,44)\| = 18$ | $\|(66,18)\| = 12$ | $\|(66,53)\| = 12$ | $\|(69,35)\| = 18$ |
| $\|(69,36)\| = 18$ | $\|\infty\| = 1$ | | | |

Por lo tanto, el punto $P = (4,5)$ con $|P| = 36$ es un elemento en $E$ con el máximo órden.

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

   *a*) ¿Es $Q = (81, -176)$ un punto de $\mathbb{E}$?
   SOLUCIÓN: Para saber si $Q$ es un punto en $E$ simplemente debemos comprobar que con los valores $x = 81$ y $y = -176$ se cumple la congruencia

$$y^2 - 2 \equiv x^3 + 333x \pmod{347}$$

   Entonces

$$\begin{aligned} y^2 - 2 &\equiv x^3 + 333x \pmod{347} \\ (-176)^2 - 2 &\equiv (81)^3 + 333(81) \pmod{347} \\ 30974 &\equiv 558414 \pmod{347} \end{aligned}$$

   Como $p = 347 \mid 558414 - 30974 = 527440$ ya que $347(1520) = 527440$, entonces podemos concluir que $Q = (81, -176) \in E(F_{347})$.

   *b*) Si sabemos que $|\mathbb{E}| = 358$. ¿Podemos decir que $\mathbb{E}$ es criptográficamente útil? ¿Cuál es el órden de $P$? ¿Entre qué valores se puede escoger la clave privada?
   SOLUCIÓN: Como $|E| = 358 = 2 \cdot 179$ entonces se puede decir que $E$ no es criptográficamente útil ya que una *curva fuerte* busca que

- El órden de $E$ sea divisible por un primo grande (2 no lo es), ó
- El órden de $E$ sea un primo grande (tenemos que 358 es par).

Utilizando la función `orden()`, definida en el ejercicio *2.c*, obtenemos que el órden del elemento $P = (110, 136)$ es 179.

Los valores de la clave privada se pueden escoger entre los enteros del intervalo $[1, 179]$, el cual está acotado por el órden del punto $P$ (ya que es el punto primitivo).

*c*) Si tu clave privada es $k = 101$ y algún conocido te ha enviado el mensaje cifrado

$$(M_1 = (232, 278), M_2 = (135, 214))$$

¿Cuál era el mensaje original?

SOLUCIÓN: El mensaje está cifrado usando *ElGamal elíptico*, por lo que simplemente hay que seguir su algoritmo para descifrar.

- Calculamos $M = M_2 - kM_1$, donde $k$ es nuestra llave privada.
  Usando la función `suma_puntos()`, implementada en el ejercicio *2.c*, obtenemos que

$$\begin{aligned} M &= (135, 214) - 101(232, 278) \\ &= (135, 214) - (275, 176) \\ &= (135, 214) + (275, -176) && \text{por definición de } -P \\ &= (74, 87) \end{aligned}$$

Por lo tanto, el mensaje original es $M = (74, 87)$.

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

   *a*) Calcula $Q = mP$.
   SOLUCIÓN: Usando la función `suma_puntos()`, implementada en el ejercicio *2.c*, obtenemos que

$$Q = 8(2, 9) = (8, 15)$$

   *b*) Descifra la siguiente cadena de texto cifrado

$$((18, 1), 21), ((3, 1), 18), ((17, 0), 19), ((28, 0), 8)$$

   SOLUCIÓN: Primero, desciframos la tupla $((18, 1), 21)$. Como $18 \in \mathbb{Z}_{31}$ y $1 \in \mathbb{Z}_2$, entonces debemos evaluar a 18 en $y^2 = x^3 + 2x + 7 \pmod{31}$. Así,

$$\begin{aligned} y^2 &= 18^3 + 2(18) + 7 \pmod{31} \\ y^2 &= 5832 + 36 + 7 \pmod{31} \\ y^2 &= 5875 \pmod{31} \\ y^2 &\equiv 16 \end{aligned}$$

   Por lo que $y = \pm 4 \pmod{31}$. Notemos que el segundo elemento de la tupla $(18, 1)$ nos dice que $y \equiv 1 \pmod{2}$, pero $-4 \equiv 27 \pmod{31}$ pero $27 \not\equiv 1 \pmod{2}$.

   *c*) Supongamos que cada texto plano representa un carácter alfabético, convierte el texto plano en una palabra en Inglés. Usa la asociación $(A \to 1, ..., Z \to 26)$.