Matemática Discreta
Grado en Ingeniería de datos - Ejercicio 2
Fecha: 30-11-2023

Apellidos y Nombre:

DNI/NIE: | | | | | | | | | |

$\underbrace{}_{A}\ \underbrace{}_{B}\ \underbrace{}_{C}\ \underbrace{}_{D}\ \underbrace{}_{E}\ \underbrace{}_{F}$

Utilizando el DNI/NIE escribir los valores de A, B y C en $\mathbb{Z}_3$ y los de D, E y F en $\mathbb{Z}_4$.

$$A = \_\_\_\_, \quad B = \_\_\_\_, \quad C = \_\_\_\_, \quad D = \_\_\_\_, \quad E = \_\_\_\_, \quad F = \_\_\_\_$$

A modo de ejemplo, si se tratase del DNI 22987657V, se tendrían los valores

$$A = 0, \quad B = 2, \quad C = 1, \quad D = 2, \quad E = 1, \quad F = 3.$$

Utilizando el código RSA explicado en el manual de prácticas se han enviado una serie de mensajes. Cada mensaje se ha etiquetado con el par (B, E) obtenidos anteriormente. Los mensajes, enviados sílaba a sílaba menos cuando las sílabas constan de más de cuatro letras en cuyo caso se envían de dos en dos letras, son los siguientes:

(0,0) Usar para descodificar $d = 541$. (e =2208061)

$$2573481 - 2897019$$

$$66756 - 4569164 - 4371188$$

(0,1) Usar para descodificar $d = 541$. (e =199761)

$$4674188 - 2820158$$

$$2942573 - 1987519$$

(0,2) Usar para descodificar $d = 541$. (e =305461)

$$798127 - 3917476$$

$$4434669 - 1121087$$

(0,3) Usar para descodificar $d = 541$. (e =1755061)

$$2324212 - 2752763 - 695692$$

$$2285313 - 1786627$$

(1,0) Usar para descodificar $d = 541$. (e =2397925)

$$3896863$$

$$4104006 - 3245600$$

(1,1) Usar para descodificar $d = 541$. (e =6001141)

$$4332203 - 2764513$$

$$4932722 - 3890545$$

(1,2) Usar para descodificar $d = 541$. (e =1746421)

$$1555359$$

$$5019971 - 4305622$$

(1,3) Usar para descodificar $d = 541$. (e =2776861)

$$3319802$$

$$2130421 - 2268393 - 4172113$$

(2,0) Usar para descodificar $d = 541$. (e =3347245)

$$959994 - 1651580$$

$$4914446 - 3300796$$

(2,1) Usar para descodificar $d = 541$. (e =1235421)

$$2302943$$

$$3029581 - 4640469$$

(2,2) Usar para descodificar $d = 541$. (e =238581)

$$3608282 - 3844792$$
$$3624194 - 1579743$$

(2,3) Usar para descodificar $d = 541$. (e =4595141)

$$55517 - 4349743$$
$$2455841 - 363582 - 3815539$$

Cada alumno debe desencriptar y proporcionar el mensaje descodificado y pasado al lenguaje con las letras correspondientes. El mensaje que tendrá que descodificar es el que se corresponda con los valores B y E obtenidos a partir de su DNI o NIE. Para poder descodificar el mensaje será preciso que obtengan los valores de los primos con los que éste se ha codificado. Estos valores se obtendran respondiendo a las dos cuestiones siguientes también dependientes de los valores B y E de cada alumno. Así, si por ejemplo $B = 1$ y $E = 2$ deberá descodificar el mensaje $(1, 2)$ respondiendo previamente a las preguntas $A1$ y $B2$.

Preguntas para la obtención de los primos

Nota. En todos los ejercicios suponemos que tenemos importado el módulo sympy y aquellos submódulos de sympy necesarios para que las sentencias introducidas en Python no den error.

A. Responder a la cuestión que corresponda:

0. Obtener el menor entero positivo x tal que

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 17), \\ x \equiv 2 (\mathrm{mod}\, 8), \\ x \equiv 13 (\mathrm{mod}\, 19). \end{cases}$$

El primo p del código RSA será el mayor número primo tal que $p \leq x$.
Solución. Tecleamos

crt([17,8,19],[1,2,13])
(1514,2584)

por lo que $x = 1514$. Tecleando ahora

$$prevprime(1514)$$

obtenemos

$$p = 1511.$$

1. Obtener el menor entero positivo x tal que

$$\begin{cases} x \equiv 1 (\mathrm{mod}\, 15), \\ x \equiv 2 (\mathrm{mod}\, 8), \\ x \equiv 13 (\mathrm{mod}\, 19). \end{cases}$$

El primo p del código RSA será el mayor número primo tal que $p \leq x$.
Solución. Tecleamos

crt([15,8,19],[1,2,13])
(1666,2280)

por lo que $x = 1666$. Tecleando ahora

$$prevprime(1666)$$

obtenemos

$$p = 1663.$$

2. Obtener el menor entero positivo x tal que

$$\begin{cases} x \equiv 5 (\mathrm{mod}\, 17), \\ x \equiv 2 (\mathrm{mod}\, 8), \\ x \equiv 13 (\mathrm{mod}\, 15). \end{cases}$$

El primo p del código RSA será el mayor número primo tal que $p \leq x$. (sol: 1858, $p = 1847$)
Solución. Tecleamos

crt([17,8,15],[5,2,13])
(1858,2040)

por lo que $x = 1858$. Tecleando ahora

$$prevprime(1858)$$

obtenemos

$$p = 1847.$$

B. Responder a la cuestión que corresponda:

0. Dado el grafo completo K_5, con vértices enumerados $V = \{1, 2, 3, 4, 5\}$. Sea $G = K_5 \setminus \{(1, 2), (3, 4)\}$. Obtener la matriz de adayacencia $\mathbf{A}$ de G y obtener a_{13} el coeficiente de la primera fila y tercera columna de la matriz

$$\mathbf{A} + \mathbf{A}^2 + \mathbf{A}^3 + \mathbf{A}^4 + \mathbf{A}^5.$$

El primo q para descifrar el mensaje será el primer primo de manera que es mayor que los $5 \cdot a_{13}$ primeros primos.
Solución. Tecleamos

A=ones(5,5)
A[0,0]=0
A[1,1]=0
A[2,2]=0
A[3,3]=0
A[4,4]=0
A[0,1]=0
A[1,0]=0
A[2,3]=0
A[3,2]=0

para construir la matriz

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

A continuación tecleamos

A+A**2+A**3+A**4+A**5

obteniendo la matriz

$$\begin{pmatrix} 87 & 87 & 98 & 98 & 115 \\ 87 & 87 & 98 & 98 & 115 \\ 98 & 98 & 87 & 87 & 115 \\ 98 & 98 & 87 & 87 & 115 \\ 115 & 115 & 115 & 115 & 140 \end{pmatrix}$$

por lo que el primo buscado se obtendrá tecleando

$$prime(5 * 98 + 1)$$

siendo éste

$$q = 3517.$$

1. Dado el grafo completo K_5, con vértices enumerados $V = \{1, 2, 3, 4, 5\}$. Sea $G = K_5 \setminus \{(1, 2), (4, 5)\}$. Obtener la matriz de adayacencia $\mathbf{A}$ de G y obtener a_{23} el coeficiente de la segunda fila y tercera columna de la matriz

$$\mathbf{A} + \mathbf{A}^2 + \mathbf{A}^3 + \mathbf{A}^4 + \mathbf{A}^5.$$

El primo q para descifrar el mensaje será el primer primo de manera que es mayor que los $5 \cdot a_{23}$ primeros primos.
Solución. Tecleamos

A=ones(5,5)
A[0,0]=0
A[1,1]=0
A[2,2]=0
A[3,3]=0
A[4,4]=0
A[0,1]=0
A[1,0]=0
A[3,4]=0
A[4,3]=0

para construir la matriz

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

A continuación tecleamos

A+A**2+A**3+A**4+A**5

obteniendo la matriz

$$\begin{pmatrix} 87 & 87 & 115 & 98 & 98 \\ 87 & 87 & 115 & 98 & 98 \\ 115 & 115 & 140 & 115 & 115 \\ 98 & 98 & 115 & 87 & 87 \\ 98 & 98 & 115 & 87 & 87 \end{pmatrix}$$

por lo que el primo buscado se obtendrá tecleando

$$prime(5 * 115 + 1)$$

siendo éste

$$q = 4211.$$

2. Dado el grafo completo K_5, con vértices enumerados $V = \{1, 2, 3, 4, 5\}$. Sea $G = K_5 \setminus \{(2, 5), (3, 4)\}$. Obtener la matriz de adayacencia $\mathbf{A}$ de G y obtener a_{43} el coeficiente de la cuarta fila y tercera columna de la matriz

$$\mathbf{A} + \mathbf{A}^2 + \mathbf{A}^3 + \mathbf{A}^4 + \mathbf{A}^5.$$

El primo q para descifrar el mensaje será el primer primo de manera que es mayor que los $5 \cdot a_{43}$ primeros primos.
Solución. Tecleamos

A=ones(5,5)
A[0,0]=0
A[1,1]=0
A[2,2]=0
A[3,3]=0
A[4,4]=0
A[1,4]=0
A[4,1]=0
A[2,3]=0
A[3,2]=0

para construir la matriz

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{pmatrix}.$$

A continuación tecleamos

A+A**2+A**3+A**4+A**5

obteniendo la matriz

$$\begin{pmatrix} 140 & 115 & 115 & 115 & 115 \\ 115 & 87 & 98 & 98 & 87 \\ 115 & 98 & 87 & 87 & 98 \\ 115 & 98 & 87 & 87 & 98 \\ 115 & 87 & 98 & 98 & 87 \end{pmatrix}$$

por lo que el primo buscado se obtendrá tecleando

$$prime(5 * 87 + 1)$$

siendo éste

$$q = 3041.$$

3. Dado el grafo completo K_5, con vértices enumerados $V = \{1, 2, 3, 4, 5\}$. Sea $G = K_5 \setminus \{(1, 2), (2, 4)\}$. Obtener la matriz de adayacencia $\mathbf{A}$ de G y obtener a_{12} el coeficiente de la primera fila y segunda columna de la matriz

$$\mathbf{A} + \mathbf{A}^2 + \mathbf{A}^3 + \mathbf{A}^4 + \mathbf{A}^5.$$

El primo q para descifrar el mensaje será el primer primo de manera que es mayor que los $5 \cdot a_{12}$ primeros primos.
Solución. Tecleamos

A=ones(5,5)
A[0,0]=0
A[1,1]=0
A[2,2]=0
A[3,3]=0
A[4,4]=0
A[0,1]=0
A[1,0]=0
A[1,3]=0
A[3,1]=0

para construir la matriz

$$A = \begin{pmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

A continuación tecleamos

A+A**2+A**3+A**4+A**5

obteniendo la matriz

$$\begin{pmatrix} 110 & 76 & 131 & 111 & 131 \\ 76 & 52 & 93 & 76 & 93 \\ 131 & 93 & 148 & 131 & 149 \\ 111 & 76 & 131 & 110 & 131 \\ 131 & 93 & 149 & 131 & 148 \end{pmatrix}$$

por lo que el primo buscado se obtendrá tecleando

$$prime(5 * 76 + 1)$$

siendo éste

$$q = 2621.$$

Mensaje descodificado

El mensaje descodificado es:

Solución. Para descodificar el mensaje tecleamos

```
n=p*q
(x**541)%n
```

donde **x** son los dígitos que queremos descodificar. Por ejemplo, con $p = 1511$ y $q = 2621$ escribimos

```
n=1511*2621
(2324212**541)%n
```

y obtenemos

1318

que se corresponde con las dos primeras letras

$$CH$$

del mensaje (0,3).