**Bifid Cypher**

1.- Describe paso a paso cómo descifrar un mensaje usando *Bifid cypher*

* Encontrar las coordenadas de cada carácter del mensaje
* Acomodar las coordenadas linealmente en el mismo orden de aparición de los caracteres
* Dividir el arreglo de números resultante a la mitad
* Acomodar la parte derecha del arreglo debajo de la parte izquierda, de manera que corresponda el primer elemento de la primera mitad con el primero de la segunda mitad; el segundo de la primera con el segundo de la segunda y así sucesivamente
* Las correspondencias anteriores corresponden a las coordenadas del carácter final. Los elementos de la primera mitad corresponden a los renglones y los de la segunda mitad a las columnas de la matriz
* Una vez halladas las coordenadas, acomodar los caracteres en el mismo orden de aparición. De esta manera se obtiene el mensaje descifrado

2.- Usar el *Bifid Cypher* con la matriz dada para lo siguiente:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | 0 | 1 | 2 | 3 | 4 |
| 0 | E | N | C | R | Y |
| 1 | P | T | A | B | D |
| 2 | F | G | H | I | K |
| 3 | L | M | O | Q | S |
| 4 | U | V | W | X | Z |

* Cifrar BRING ALL YOUR MONEY

Encontramos las coordenadas de cada letra y las acomodamos en dos renglones. Arriba los renglones y abaja las columnas

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| B | R | I | N | G | A | L | L | Y | O | U | R | M | O | N | E | Y |
| 1 | 0 | 2 | 0 | 2 | 1 | 3 | 3 | 0 | 3 | 4 | 0 | 3 | 3 | 0 | 0 | 0 |
| 3 | 3 | 3 | 1 | 1 | 2 | 0 | 0 | 4 | 2 | 0 | 3 | 1 | 2 | 1 | 0 | 4 |

Concatenamos la parte correspondiente a las columnas al final de la cadena correspondiente a los renglones.

**1020213303403300033311200420312104**

Ahora agrupamos la cadena resultante cada dos elementos, los cuales corresponderán a las coordenadas del nuevo carácter que conformará el mensaje de salida

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 10 | 20 | 21 | 33 | 03 | 40 | 33 | 00 | 03 | 33 | 11 | 20 | 04 | 20 | 31 | 21 | 04 |
| P | F | G | Q | R | U | Q | E | R | Q | T | F | Y | F | M | G | Y |

Finalmente el mensaje resultante después del cifrado es el siguiente:

**PFGQRUQERQTFYFMGY**

* Descifrar PDRRNGBENOPNIAGGF

Encontramos las coordenadas de cada uno de los caracteres del mensaje y los acomodamos linealmente

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| P | D | R | R | N | G | B | E | N | O | P | N | I | A | G | G | F |
| 10 | 14 | 03 | 03 | 01 | 21 | 13 | 00 | 01 | 32 | 10 | 01 | 23 | 12 | 21 | 21 | 20 |

El arreglo resultante lo dividimos a la mitad y alineamos la parte izquierda con la parte derecha, de tal manera que las posiciones de cada subcadena correspondan. Con lo anterior, cada pareja de números corresponderá a las coordenadas del carácter descifrado.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 0 | 1 | 4 | 0 | 3 | 0 | 3 | 0 | 1 | 2 | 1 | 1 | 3 | 0 | 0 | 0 |
| 1 | 3 | 2 | 1 | 0 | 0 | 1 | 2 | 3 | 1 | 2 | 2 | 1 | 2 | 1 | 2 | 0 |
| T | R | A | V | E | L | N | O | R | T | H | A | T | O | N | C | E |

Finalmente, el mensaje descifrado es el siguiente:

**TRAVELNORTHATONCE**

3.- Crear el pseudo-código para las funciones de cifrado y descifrado del *Bifid Cypher*

**Leer** la llave para el proceso

**Generar** la matriz del *Bifid Cypher* a partir de la llave dada

* Para descifrar

1. **Leer** el mensaje a descifrar
2. **Encontrar** las coordenadas de cada carácter y almacenarlas en un arreglo lineal
3. **Calcular** las coordenadas de los caracteres de salida con ayuda de los índices
   * Las coordenadas están definidas por **( coord(i) , coord(n/2+i) )**
   * ***i:*** índice de cada número de la cadena del paso 2. *0 ≤ i ≤ n/2*
   * ***n:*** longitud de la cadena del paso 2
4. **Obtener** los caracteres descifrados a partir de las coordenadas del paso 3
5. **Concatenar** los caracteres obtenidos del paso anterior
6. **Mostrar** el mensaje descifrado

* Para cifrar

1. **Leer** mensaje a cifrar
2. **Encontrar** las coordenadas de cada carácter y almacenarlas en un arreglo lineal
3. **Calcular** las coordenadas de los caracteres de salida con ayuda de los índices

* Las coordenadas de los caracteres están dadas por **(coord(i), coord(i+2))**
* Para la primera mitad: *0 ≤ i < n*, *i = 0, 4, 8, 12,…*
* Para la segunda mitad: *1 ≤ i < n*, *i = 1, 5, 9, 13,…*
* ***n:*** longitud de la cadena del paso 2

1. **Obtener** los caracteres cifrados con las coordenadas del paso 3
2. **Concatenar** los caracteres del paso 4
3. **Mostrar** el mensaje cifrado

4.- Implementar el pseudo-código anterior en el lenguaje de preferencia