Miramontes Sarabia Luis Enrique

23 de agosto del 2019

PRÁCTICA 1: BIFID CIPHER

DECRIBE STEP BY STEP HOW YOU CAN DECRYPT A MESSAGE USING THE BIFID CIPHER

1. Tomando el cipher text y usando la misma tabla usada para cifrar encontramos los índices de cada carácter del cipher text. Ejemplo: “LNLLFGPPNPGRSK” -> “3001303020211010011021033424”

2. Se divide la cadena de índices a la mitad, creando dos cadenas de la misma longitud.

Ejemplo: “3001303020211010011021033424” -> ”30013030202110” “10011021033424”

3. Se concatenan cada uno de los caracteres de cada cadena resultante con el respectivo homólogo del mismo índice de la otra cadena.

Ejemplo: ”30013030202110” + “10011021033424” -> “31 00 00 11 21 00 23 01 20 03 23 14 12 04”

4. Usar los índices obtenidos para encontrar el equivalente de los índices en letras.

Ejemplo: “31 00 00 11 21 00 23 01 20 03 23 14 12 04” - > “M E E T M E O N F R I D A Y”

USE THE BIFID CIPHER WITH THE TABLEAU AS GIVEN TO

Encrypt “BRING ALL YOUR MONEY”

“BRING ALL YOUR MONEY” -> “13 03 23 01 21 12 30 30 04 32 04 03 31 32 01 00 04” -> “10202133034033000333112004203121 04” -> “10 20 21 33 03 40 22 00 03 33 11 20 04 20 31 21 04” -> “PFGQRUQUERQTFYFMGY”

Decrypt “PDRRNGBENOPNIAGGF”

“PDRRNGBENOPNIAGGF” -> “10 14 03 03 01 21 13 00 01 31 10 01 23 12 21 21 20” -> “11 03 12 41 00 30 01 32 03 11 22 12 11 32 01 02 00” -> “TRAVELNORTHATONCE”

PSEUDOCODE

+Llenado de la tabla

1. Leer las entradas: LLAVE e INTEXT
2. Declarar una matriz TABLA de 5x5
3. Meter a una matriz de 5x5 los caracteres que contiene la llave
4. Terminar de rellenar la matriz de 5x5 con letras en orden alfabético y sin repetir.

+Cifrado

1. Declarar dos arreglos nuevos cypher_L y cypher_H
2. FOR cada elemento en INTEXT:
    2.1 Añadir a cypher_L el número de fila donde se encuentra el elemento en la tabla
    2.2 Añadir a cypher_H el número de columna donde se encuentra el elemento en la tabla
3. Declarar un nuevo arreglo cypher_HL
4. Concatenar cypher_H + cypher_L y guardarlo en cypher_HL
5. Declarar un nuevo arreglo cyphertext
6. FOR index < longitud de cypher_l
    5.1 Tomar los primeros dos elementos de cypher_HL y emplearlos como índice de renglón y columna de la matriz TABLA respectivamente.
    5.2 Guardar el elemento almacenado en la localidad de la matriz TABLA en cyphertext
7. Mostrar cyphertext

+Descifrado

1. Declarar un arreglo decrypt y otro llamdo plaintext
2. For cada elemento en INTEXT:
    3.1 Buscar el elemento dentro de la matriz TABLA
    3.2 Almacenar el índice correspondiente a la fila en decryp
    3.3 Almacenar el índice correspondiente a la columna en decrypt
3. For index < (longitud decrypt)/2
    3.1 Obtener el elemento de la matriz TABLA cuyos índices son decrypt[index] para renglón y decrypt[index+ ((longitud decrypt)/2)]
    3.2 Añadir el elemento obtenido a plaintext
4. Mostrar plaintext

CODE

The code was uploaded to Alphagrader and developed with Python 3.6.5