Grado en Ingeniería Informática

Especialidad de Computación

Cuarto curso, Primer cuatrimestre

Curso académico: 2020-2021

Códigos y Criptografía

Práctica: Cifra ADFGVX

1. **Función matriz = init_matrix(publica)**

Función que se encarga de inicializar la matriz de cifrado a partir de una clave pública. Para ello, se recomienda convertir la clave a letras mayúsculas así como el abecedario utilizado.

Entradas:

- *publica*: Es la clave pública a partir de la cual generaremos la matriz de cifrado.

Salidas: como salida obtendremos un matriz de cifrado cuadrada de dimensión 6 x 6.

Ejemplo:

```
>> init_matrix('hoy hace un buen dia')

ans =

  6×6 char array

    'HOYACE'
    'UNBDIF'
    'GJKLMP'
    'QRSTVW'
    'XZ0123'
    '456789'
```

2. **Función cadena_sust = sustitucion(matriz, mensaje)**

Función que se encarga de realizar la sustitución de cada carácter del mensaje por su correspondiente pareja de letras utilizando la cifra ADFGVX.

Entradas:

- *matriz*: matriz de cifrado cuadrada de dimensión 6 x 6.
- *mensaje*: cadena de caracteres que queremos sustituir haciendo uso de la matriz mencionada.

Salidas: como salida obtendremos la cadena resultante de sustituir cada carácter por su par de letras cifradas.

Ejemplo:

```
>> matriz = init_matrix('hoy hace un buen dia');
>> sustitucion(matriz,'comenzamos la practica')

ans =

    'AVADFVAXDDVDAGFVADGFFGAGFXGDAGAVGGDVAVAG'
```

3. **Función mensaje_cifrado = cifrado(mensaje, publica, privada)**

Función que se encarga de obtener un mensaje cifrado utilizando el método ADFGVX.

Entradas:

- *mensaje*: cadena de caracteres que queremos cifrar haciendo uso del método ADFGVX.
- *publica*: clave a partir de la cual crearemos la matriz de cifrado.
- *privada*: clave privada con la que se realizarán las permutaciones correspondientes para el cifrado.

Salidas: como salida obtenemos el mensaje cifrado.

Ejemplo:

```
>> cifrado('comenzamos la practica','hoy hace un buen dia','uco')

ans =

    'VFXVGAFAXAVDVXAVDDFDFGGGGVAXADADAVGGFDAGAG'
```

4. **Función des_mensaje = deshacer_sustitucion(matriz, mensaje)**

Función que deshace la sustitución de un carácter por dos caracteres de la cifra ADFGVX.

Entradas:

- *matriz*: matriz de descifrado que se utilizará para obtener el mensaje descifrado.
- *mensaje*: mensaje cifrado que queremos descifrar usando la matriz de descifrado.

Salidas: como salida obtenemos el mensaje correctamente descifrado

Ejemplo:

```
>> matriz=init_matrix('hoy hace un buen dia');
>> sustituido=sustitucion(matriz,'comenzamos la practica');
>> deshacer_sustitucion(matriz,sustituido)

ans =

    'COMENZAMOSLAPRACTICA'
```

5. **Función mensaje_des = descifrado(mensaje, publica, privada)**

Función que descifra un mensaje cifrado utilizando las claves privada y pública.

Entradas:

- *mensaje*: mensaje cifrado que queremos descifrar.
- *publica*: clave con la cual construiremos la matriz de descifrado.
- *privada*: clave privada con la que se realizarán las permutaciones correspondientes para el descifrado.

Salidas: como salida obtenemos el mensaje descifrado.

Ejercicio:

Para terminar con la práctica deberemos comprobar que el mensaje descifrado obtenido para las siguientes entradas es coherente y nos lleva al lugar indicado. Las entradas para este ejercicio son:

- *mensaje:*
  'VDFAFAVAXGXGAAFDADFAGDAXAGGXDDGFDDDVAVDVDXDAAAVGGG'
- *publica:* 'franberchez'
- *privada:* 'oculto'