Proyecto 1 “ Cifrado César”

Objetivos

- El alumno aprenderá a crear comandos a partir de shell script
- El alumno aprenderá a crear un man page.

Introducción

En criptografía, el cifrado César, también conocido como cifrado por desplazamiento, es una de las técnicas de cifrado más simples y más usadas. Es un tipo de cifrado por sustitución en el que una letra en el texto original es reemplazada por otra que se encuentra un número fijo de posiciones más adelante en el alfabeto.

Recursos utilizados

Arreglos en bash script

Declaración de arreglos

Cuando se conocen los elementos del arreglo se puede declarar e inicializar al mismo tiempo de las siguientes formas:

```
letras=(a b c d e)

declare -a letras=(a b c d e)
```

Cuando no se conocern los elementos se puede declarar de la siguiente manera:

```
numeros=()
```

Y para inicializarlo o agregar elementos:

```
numeros[0]=1
numeros[1]=1
numeros[2]=2
```

Para acceder al valor de un elemento:

```
echo ${numeros[2]}
```

Para saber el tamaño del arreglo:

```
echo ${#numeros[@]}
```

Para imprimir todos los elementos de un arreglo:

```
echo ${#numeros[*]}
```

Convertir una cadena a un arreglo
Se declara un arreglo, con ayuda de la sentencia ${#cadena} se obtiene la longitud de la cadena que queremos convertir en un arreglo, pero como sabemos los indices de un arreglo comienzan en 0, por lo que le restamos una unidad de modo que guarde todos los caracteres de la cadena. Esto se logra por medio de un ciclo for y de una secuencia, se le asigna a cada elemento del arreglo un carácter de la cadena, se secciona la cadena con ${cadena:$i:1}

```
array=()
for i in $(seq 0 $((${#cadena} - 1)));
do
        array[i]=${cadena:$i:1}
done
```

Borrar elementos de un arreglo
Para eliminar tanto un arreglo como alguno de sus elementos

```
unset numeros[0]

unset numeros
```

Archivos

Leer linea por linea un archivo

```
while IFS='' read -r linea || [[ -n "$linea" ]];
do
    echo $linea
done < fichero
```

IFS=' ' (o IFS=) impide que se eliminen los caracteres de espacio (espacio o tabulador) iniciales o finales.
-r impide que la contrabarra (\) se interprete como un carácter especial.
|| [[-n $linea]] impide que se ignore la última línea si no termina con \n (pues read devuelve un exit no-cero cuando encuentra un EOF).

Eliminar el contenido de un archivo

Se puede eleminar el contenido con alguna de la siguientres tres formas:

```
true > archivo

cat /dev/null > fichero

echo "" > fichero
```

Concatenar lineas a un archivo

Concatena lineas al final del archivo

```
echo $texto >> $archivo
```

Como ejecutar un script dentro de otro script

Se puede ejecutar un script dentro de otro script con alguna de la siguientres tres formas:

```
source archivo.sh

. archivo.sh

source archivo.sh
```

Desarrollo

Después de haber instalado el comando se podra ejecutar de la siguiente manera

ec – e archivo → Para encriptar
ec – d archivo → Para desencriptar
ec – x script.sh → Para ejecutar un script encriptado

Adicionalmente se le podran poner otras dos banderas

– s numero → para cambiar el desplzamiento
– a abecedario → para cambiar el abecedario

Por defeecto el programa tiene un desplazamiento de 4 y el abecedario incluye de a la A-Z y a-z.

El programa comienza leyendo las banderas y los parametros de cada una de ellas, según sea la bandera se le asigna un numero de caso, en caso de se cambie el

desplazamiento se le asigna el nuevo valor a la variable que almacena el valor del dezplazamiento, e igual si se propone un nuevo abecedario.
Después con ayuda de un case se realizan las operaciones correspondientes para caso.

- **Encriptar**

  Se crea un archivo auxiliar al cual se le pasa el contenido del archivo original, pero se le sustituyen los espacios por un simbolo, esto se hace para que respeten los espacios y las tabulaciones, despues se vacia el archivo original, y se lee linea por linea del archivo auxiliar, para cada linea se invoca la funcion encriptar, la cual hace el desplazamiento pedido con el abecedario especificado, luego de eso se guarda la linea en el archivo original sustituyendo el simbolo por espacios para que quede de la misma forma.
  Al finalizar este proceso se elimina el archivo auxiliar.

- **Desencriptar**

  Para desencriptar se deben tener en consideración que se debe hacer con el desplazamiento y con el abecedario con el que se encripto.

  Se crea un archivo auxiliar al cual se le pasa el contenido del archivo original, pero se le sustituyen los espacios por un simbolo, esto se hace para que respeten los espacios y las tabulaciones, despues se vacia el archivo original, y se lee linea por linea del archivo auxiliar, para cada linea se invoca la funcion desencriptar, la cual deshace el desplazamiento pedido con el abecedario especificado, luego de eso se guarda la linea en el archivo original sustituyendo el simbolo por espacios para que quede de la misma forma.
  Al finalizar este proceso se elimina el archivo auxiliar.

- **Ejecutar**

  Para ejecutar un script encriptado el script no debe contener errores, asi como también se debe tener en consideración el desplazamiento y el abecedario con el que se encripto.

  Se crean dos archivos auxiliares, uno de ellos es vacio y el otro se le pasa el contenido del archivo original, pero se le sustituyen los espacios por un simbolo, esto se hace para que respeten los espacios y las tabulaciones, se lee linea por linea del archivo auxiliar 1, para cada linea se invoca la funcion desencriptar, la cual deshace el desplazamiento pedido con el abecedario especificado, luego de eso se guarda la linea en el archivo auxiliar 2 sustituyendo el simbolo por espacios para que quede de la misma forma.
  Al finalizar este proceso se tendra que el archivo auxiliar 2 contendra el contenido que se desea ejecutar, el archivo auxiliar 2 se ejecuta y al finalizar los dos archivos auxiliares se eliminan.

Referencias

Arrays en bash. abril 13, 2019, de a Sitio web: https://gulvi.com/serie/curso-programacion-bash/capitulo/arrays-bash

¿Cómo agregar / eliminar un elemento de / a la matriz en bash?. abril 13, 2019, de a Sitio web: http://linux.dokry.com/cmo-agregar-eliminar-un-elemento-de-a-la-matriz-en-bash.html

¿Cómo puedo leer contenido de un fichero?. abril 13, 2019, de a Sitio web: https://es.stackoverflow.com/questions/129805/c%C3%B3mo-puedo-leer-el-contenido-de-un-fichero-l%C3%ADnea-a-l%C3%ADnea-con-bash

Cómo vaciar ficheros en Linux. abril 14, 2019, de a Sitio web: http://rm-rf.es/como-vaciar-ficheros-en-linux/