Universidad Nacional De Asunción

FACULTAD POLITÉCNICA

Lenguajes de Programación III – Primer Examen Final – 17/11/2021 – 1 hora de tiempo

Test de Programación Bash - Cifrado Playfair

El Cifrado Playfair permite cifrar un texto por medio de la sustitución de "digramas" (agrupaciones de 2 letras), utilizando tradicionalmente para realizar el cifrado y el descifrado una cuadrícula de letras revueltas y no repetidas de 5 x 5.

En la cuadrícula, cada letra del alfabeto debe aparecer una sola vez y para que la misma sea cuadrada, normalmente la "I" representa indistintamente a sí misma y a la "J" y la “N”, a sí misma y a la “Ñ”. Para construir la cuadrícula, una clave elegida arbitrariamente aparece primero, por ejemplo "CODES", y luego, se completa el resto del alfabeto en orden, de izquierda a derecha, salteándose las letras ya utilizadas.

```
C O D E S
A B F G H
I K L M N
P Q R T U
V W X Y Z
```

Para realizar el cifrado o el descifrado, un mensaje en texto claro se divide en digramas, obviando los espacios. Si un digrama con tiene dos letras idénticas se debe borrar la segunda y formar un nuevo digrama con la siguiente letra del mensaje. Si al final queda una sola letra, se complementa con un carácter "nulo", típicamente una "X". Así, el texto:

```
THIS IS A TOP SECRET MESSAGE
```

se convierte en:

```
TH IS IS AT OP SE CR ET ME SA GE
```

Para realizar cifrado, cada diagrama se procesa de acuerdo a tres posibilidades:

1) Si ambas letras estarán en la misma fila de la cuadricula, cada letra se sustituye por aquella que está inmediatamente a su derecha. Si es necesario, debe considerarse volver al principio de la fila.

2) Si ambas letras estarán en la misma columna de la cuadricula, cada letra se sustituye por aquella la que está inmediatamente debajo de ella. Si es necesario, debe considerarse volver a la parte superior de la columna.

3) Sino, ambas letras formarán las esquinas de un (sub-) rectángulo dentro de la cuadricula. Cada letra se sustituye por la letra de la esquina del rectángulo que se encuentra en la misma fila.

Por ejemplo:

a. El digrama "TH" cae en el caso 3, siendo el rectángulo el siguiente:

```
G H
M N
T U
```

de esta forma, la “T” se sustituye por la “U” y la “H” por la “G”.

b. El digrama "SE" cae en el caso 1. La primera fila contiene la "S" y la "E":

```
C O D E S
```

de esta forma, la “S” se sustituye por la “C” y la “E” por la “S”.

Para descifrar el texto cifrado, se aplica la sustitución inversa en cada caso, es decir las sustituciones se realizan en sentido opuesto.

Se pide:

Desarrolle un Script Bash que implemente el Cifrado Playfair, tal que el mismo reciba tres argumentos:

1. La Clave a usar
2. La acción a realizar, por ejemplo `-c --cifrar` o `-d --decifrar`
3. Un mensaje a cifrar

Por ejemplo:

```
$> playfair CODES -c “THIS IS A TOP SECRET MESSAGE”
El mensaje cifrado es: “UGNCNCGPCQCSDPGYTGCHMG”

$> playfair CODES -d “UGNCNCGPCQCSDPGYTGCHMG”
El mensaje descifrado es: “THISISATOPSECRETMESAGE”
```

El script resultante debe hacer uso intensivo de arrays y funciones, además debe estar debidamente comentado e indentado para que su código pueda ser evaluado más allá de que el Script sea funcional.