

Guía 5: Encriptación.

Objetivos

- **Conocer que es la encriptación y como implementarla usando clases.**
- **Aprender a desarrollar diversos algoritmos de encriptación.**

¿Qué es encriptación?:

Es el proceso para volver ilegible información considera importante.

Dado esto podemos decir la encriptación es una forma de preservar la seguridad de los datos, la encriptación se utiliza mucho en variables que son de suma importancia, ya sea en bancos, hospitales, áreas de seguridad militar, etc.

Dado esto, a lo largo de la humanidad se desarrollaron muchas maneras de encriptar ya sea palabras, números, coordenadas, cada una mejor que la anterior.

Cifrado de Verman:

“El cifrado Vernam es un algoritmo de criptografía inventado por Gilbert Vernam, ingeniero AT&T Bell Labs, en 1917.

En terminología moderna, un cifrado de Vernam es un cifrado de flujo en el que el texto en claro se combina, mediante la operación XOR, con un flujo de datos aleatorio o pseudoaleatorio del mismo tamaño, para generar un texto cifrado.

El uso de datos pseudoaleatorios generados por un generador de números pseudoaleatorios criptográficamente seguro es una manera común y efectiva de construir un cifrado en flujo.”

En pocas palabras es un cifrado que utiliza una llave que puede ser generada de manera aleatoria del mismo tamaño que la palabra a encriptar y la operación XOR para generar un resultado encriptado.

Ejemplo:

Paso 1:

Se desea encriptar la palabra “hola” la cual se conoce que tiene longitud 4.

Palabra = “hola”

Longitud = 4

Programación II

Luego se genera una llave totalmente aleatoria que puede ser "M97G".

Llave = M97G

La llave posee la misma longitud que la palabra, y posee una combinación de números y letras, además puede contener caracteres validos entendibles del código ASCII, por lo que tanto la llave y el resultado no necesariamente tendrá que ser una palabra, sino una serie de caracteres del código ASCII.

Paso 2:

Es necesario tratar cada carácter de la palabra y de la llave forma individual y pasarlo a su respectivo valor decimal en ASCII.

h = 104	M = 77
o = 111	9 = 57
l = 108	7 = 55
a = 97	G = 71

Luego de esto se procede a aplicar operaciones binarias (bit a bit en c++) para cada uno de los caracteres, la operación será la función XOR.

h=	104	= 1101000	
m=	77	= <u>1001101</u>	
		0100101	=37 =%
o=	111	= 1101111	
9=	57	= <u>0111001</u>	
		1010110	=86 =V
l=	108	= 1101100	
7=	55	= <u>0110111</u>	
		1011011	=91 =[
a=	97	= 1100001	
G=	71	= <u>1000111</u>	
		0100110	=38 =&

Por lo que el resultado de encriptar la palabra **hola** es **%V[&** como la palabra encriptada usando la llave **M97G**.

Des encriptación:

Paso 1:

La des encriptación es el proceso inverso de la encriptación, por lo que recibimos como parámetro una cadena encriptada y una llave, con esto realizamos los pasos contrarios a la encriptación para retornar la palabra original.

Encriptado = %V[&
Llave = M97G

Paso 2:

Convertir cada carácter de la cadena encriptada y la llave a su equivalente numérico en ASCII, además de realizar la operación XOR para cada uno de los caracteres.

%=	37	= 0100101	
m=	77	= <u>1001101</u>	
		1101000	=104 =h
V=	86	= 1010110	
9=	57	= <u>0111001</u>	
		1101111	=111 =o
[=	91	= 1011011	
7=	55	= <u>0110111</u>	
		1101100	=108 =l
&=	38	= 0100110	
G=	71	= <u>1000111</u>	
		1100001	=97 =a

Por lo que el resultado es nuestra palabra original **hola**.

Programación II

Implementación en c++:

Con el algoritmo concluido procedemos a crear nuestras clases para manejar las diferentes operaciones de encriptación, des encriptación y los atributos que esta posee.

Encriptador
- palabra: string - llave: string - resultado: string
+ Encriptador() + Cifrado_verman(string): void + Descripta_verman(string,string): void + getPalabra(): string + getLlave(): string + getResultado(): string + modulo(int,int): int

- Encriptador(): constructor que inicializa los string palabra,llave y resultado, como una cadena vacia.
- Cifrado_verman(string): recibe como parámetro la palabra a encriptar, realiza el proceso de generar la llave y el resultado, además de guardarlos en los atributos correspondiente, muestra el resultado final.
- Descripta_verman(string,string): recibe como primer parámetro la palabra encriptada, como segundo la llave, y realiza la operación para encontrar la palabra original.
- getPalabra(): retorna el string palabra.
- getLlave(): retorna el string llave.
- getResultado(): retorna el string resultado.
- modulo(int,int): realiza la operación matemática para el módulo de la división.

```
int Encriptador::modulo(int a,int b){  
    int d =a/b;  
    return a-(d*b);  
}
```

Programación II

Operaciones bit a bit en c++:

- **&** : operador **AND** compara cada bit del primer operando con el segundo operando, si ambos bit son 1 retorna 1 de lo contrario es 0.

```
int a=5,b=3;
int r = a&b;
cout << "\nr : "<< r;//retorna 1
```

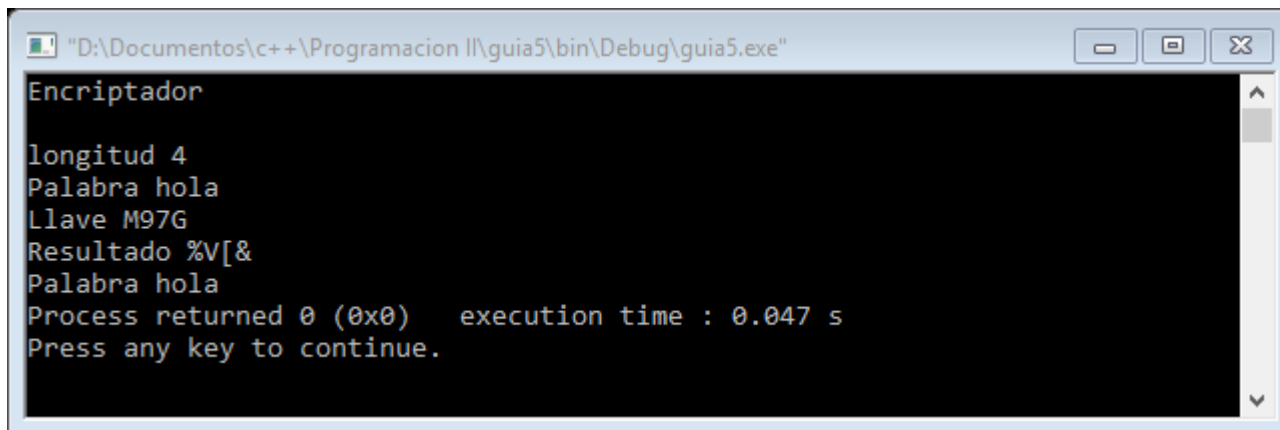
- **^** : operador **XOR** compara cada bit de su primer operando con el bit correspondiente de su segundo operando. Si un bit es 0 y el otro bit es 1, el bit del resultado correspondiente se establece en 1. De lo contrario, el bit del resultado correspondiente se establece en 0.

```
int a=5,b=3;
int r = a^b;
cout << "\nr : "<< r;//retorna 6
```

- **|** : operador **OR** compara cada bit de su primer operando con el bit correspondiente de su segundo operando. Si uno de los dos bits es 1, el bit del resultado correspondiente se establece en 1. De lo contrario, el bit del resultado correspondiente se establece en 0.

```
int a=5,b=3;
int r = a|b;
cout << "\nr : "<< r;//retorna 7
```

Resultado:



```
"D:\Documentos\c++\Programacion II\guia5\bin\Debug\guia5.exe"
Encriptador

longitud 4
Palabra hola
Llave M97G
Resultado %V[&
Palabra hola
Process returned 0 (0x0) execution time : 0.047 s
Press any key to continue.
```

Programación II

Ejercicios:

- Completar los métodos de la clase Encriptador e implementarlo.
- Construir un menú para las operaciones de encriptación y opción salir.
- Agregar dos funciones a la clase Encriptador donde desarrolle su propio algoritmo de encriptación así como su función para desencriptar. Para este ejercicio puede adaptar un algoritmo de internet o puede crear uno.