

Luis Rodolfo Nájera Ramírez

Bonjoursoft

Duración total del curso: 20 horas

Horarios:

Sábados 10:00-15:00 hrs

## **Curso: Introducción a la Criptografía: “El poder de los cifrados”**

¿Por qué es necesario proteger la información?, ¿Es posible que la información pueda volverse totalmente confidencial?, ¿Cómo puedo lograr proteger la información importante de mis sistemas?

En el curso Introducción a la criptografía: "El poder de los cifrados", daremos respuesta a estas preguntas. Inscríbete y aprende a implementar los algoritmos clásicos de criptografía Mono alfabética, Poli alfabética, Simétrica y Asimétrica.

### **TEMARIO:**

1. Introducción a la criptología
  - 1.1 Criptografía
  - 1.2 Esteganografía
  - 1.3 Criptoanálisis
  - 1.4 Estegoanálisis
2. Introducción a la criptografía
  - 2.1 Historia de la Criptografía
    - 2.1.1 Egipto
    - 2.1.2 Grecia
    - 2.1.3 Hebreos
    - 2.1.4 Espartanos
    - 2.1.5 Maquina Enigma
    - 2.1.6 Actualidad
  - 2.2. Cifrar vs Encriptar
    - 2.2.1 Definición de cifrar y encriptar
    - 2.2.2 Errores comunes
  - 2.3 La importancia de cifrar la información
4. Legislación Informática
  - 4.1 Leyes de criptografía en el mundo
    - 4.1.1 Leyes de criptografía en Europa
    - 4.1.2 Estados unidos y la criptografía
    - 4.1.3 Leyes de criptografía en México
5. Bases y Principios Básicos de programación
  - 5.1 Principios Básicos
    - 5.1.1 Partes de un programa
    - 5.1.2 Variables y constantes
    - 5.1.3 Operadores Básicos
      - 5.1.3.1 Suma
      - 5.1.3.2 Resta
      - 5.1.3.3 Multiplicación
      - 5.1.3.4 División
      - 5.1.3.5 Modulo
  - 5.2 Estructuras de control básicas
    - 5.1.1 Switch
    - 5.1.2 If
    - 5.1.3 Else
    - 5.1.4 While
    - 5.1.5 For

Luis Rodolfo Nájera Ramírez

Bonjoursoft

Duración total del curso: 20 horas

Horarios:

Sábados 10:00-15:00 hrs

- 5.1.6 Do While
- 5.3 Manejo de cadenas
  - 5.3.1 Arreglo de caracteres
  - 5.3.2 Apuntadores
  - 5.3.3 Tamaño de una cadena
  - 5.3.3 Recorriendo cadenas
  - 5.3.4 String.h
  - 5.3.5 Strings
- 5.4 Manejo de funciones
- 5.5 Lógica booleana
  - 5.5.1 And
  - 5.5.2 Or
  - 5.5.3 Xor
  - 5.5.4 Not
- 5.6 Operadores lógicos y manejo de bits
  - 5.6.1 And
  - 5.6.2 Or
  - 5.6.3 Xor
  - 5.6.4 Not
  - 5.6.5 Recorrimiento de bits
- 5.7 Teoría de números
  - 5.7.1 Números primos
  - 5.7.2 MCD, MCM
  - 5.7.3 Algoritmo de Euclides
  - 5.7.4 Bases numéricas
  - 5.7.5 Algoritmo de la división
- 6. Cifrados por sustitución mono-alfabética
  - 6.1 Cifrado Atbach
  - 6.2 Cifrado Cesar
- 7. Cifrados por sustitución Poli-alfabética
  - 7.1. Cifrado Vigenere
  - 7.2 Cifrado por transposición
- 8. Cifrados Simétricos
  - 8.1 Feistel
  - 8.2 Des
  - 8.3 Triple Des
- 9. Cifrados Asimétricos
  - 9.1 RSA
- 10. Conocimientos básicos en la industria.
- 11. El futuro de la criptografía
- 12. Buenas prácticas para proteger la información.