

## Índice de contenidos

|   |       |
|---|-------|
| RESUMEN EJECUTIVO .....   | 1-I   |
| AGRADECIMIENTOS.....  | 1-III |
| ÍNDICE DE CONTENIDOS.....                                       | 1-IV  |
| ÍNDICE DE TABLAS.....   | 1-VI  |
| ÍNDICE DE FIGURAS .....   | 1-VII |
| 1 INTRODUCCIÓN.....   | 1-1   |
| 1.1 ¿Por qué es importante la seguridad de la información?..... | 1-2   |
| 2 CONCEPTOS PRELIMINARES.....                                   | 2-5   |
| 2.1 Conceptos matemáticos previos.....                          | 2-6   |
| 2.2 Números enteros y propiedades .....                         | 2-7   |
| 2.3 Teoría de la Complejidad.....                               | 2-12  |
| 2.4 Algoritmos en $\mathbb{Z}$ .....                            | 2-16  |
| 2.5 Los enteros módulo $n$ .....                                | 2-18  |
| 2.6 Álgebra Abstracta.....                                      | 2-23  |
| 2.7 Funciones .....   | 2-28  |
| 2.7 Permutaciones .....   | 2-31  |
| 2.8 Involuciones .....  | 2-32  |
| 3 PREÁMBULO A LA CRIPTOGRAFÍA .....                             | 3-33  |
| 3.1 Seguridad de la Información y Criptografía.....             | 3-34  |
| 3.2 Definición de Criptografía.....                             | 3-37  |
| 3.3 Terminología básica y conceptos .....                       | 3-39  |
| 3.4 Logrando la confidencialidad .....                          | 3-41  |
| 3.5 Comunicación entre los participantes.....                   | 3-42  |

---

|   |      |
|---|------|
| 3.6 Canales .....   | 3-43 |
| 3.7 Seguridad .....   | 3-44 |
| 3.8 Seguridad de la Información en general .....                                  | 3-44 |
| 3.9 Criptología .....   | 3-45 |
| 4 ENCRIPCIÓN DE CLAVE PÚBLICA .....   | 4-47 |
| 4.1 Introducción y panorama general .....   | 4-48 |
| 4.2 Encriptación de clave pública RSA .....                                       | 4-51 |
| 4.3 Seguridad del algoritmo RSA .....   | 4-54 |
| 4.4 Las funciones hash .....  | 4-58 |
| 4.5 Certificados de clave pública .....   | 4-59 |
| 5 ENCRIPCIÓN DE CLAVE SIMÉTRICA .....   | 5-60 |
| 5.1 Definición y conceptos previos .....  | 5-61 |
| 5.2 Cifrado de Bloques .....  | 5-63 |
| 5.3 Carácter práctico y la complejidad de los ataques .....                       | 5-64 |
| 5.4 Criterios para la evaluación de cifrado de bloques y modos de operación ..... | 5-66 |
| 5.5 Búsqueda exhaustiva de claves y cifrados múltiples .....                      | 5-74 |
| 5.6 DES .....   | 5-76 |
| 5.7 RC5 .....   | 5-80 |
| 6 CIFRADOS CLÁSICOS Y COMPUTACIÓN CUÁNTICA .....                                  | 6-82 |
| 6.1 Sistemas de cifrados clásicos y desarrollo histórico .....                    | 6-83 |
| 6.2 Máquinas de cifrados polialfabéticos .....                                    | 6-86 |
| 6.3 Redundancias .....  | 6-89 |
| 6.4 Computación cuántica .....  | 6-90 |

|                      |      |
|----------------------|------|
| 7 CONCLUSIONES.....  | 7-93 |
| 8 BIBLIOGRAFÍA ..... | 8-97 |

## Índice de Tablas

|  |      |
|--|------|
| Tabla 1.1 - Complejidad Binaria de las cuatro operaciones básicas. ....  | 2-16 |
| Tabla 1.2 - Pasos del algoritmo Euclidiano extendido. ....               | 2-18 |
| Tabla 1.3 - El orden de algunos elementos de $\mathbb{Z}_{21}^*$ .....   | 2-21 |
| Tabla 1.4 - Potencias de $\alpha$ módulo 13 .....                        | 2-21 |
| Tabla 1.5 - Los subgrupos de $\mathbb{Z}_{19}^*$ y sus generadores. .... | 2-26 |
| Tabla 1.6 - Valores para la función $f(x) = r_x$ . ....                  | 2-30 |
| Tabla 1.7 - Objetivos relacionados a la seguridad de la información..... | 3-35 |

## Índice de Figuras

|  |      |
|--|------|
| Figura 1.1 -Regla entre los conjuntos $X = \{a, b, c\}, Y = \{1,2,3,4\}$ .....                                   | 2-29 |
| Figura 1.2 -Esquema entre las funciones $f$ y $g$ .....  | 2-30 |
| Figura 1.3 -Ejemplo de una involución .....  | 2-32 |
| Figura 1.4 -Las seis posibles encriptaciones $E_i$ .....   | 3-41 |
| Figura 1.5 -Modelo de comunicación bilateral.....  | 3-42 |
| Figura 1.6 -Comunicación entre dos partes usando un cifrado, con un canal seguro y una clave intercambiada ..... | 5-62 |
| Figura 1.7 - Modo de Operación ECB.....  | 5-68 |
| Figura 1.8 - Modo de Operación CBC. ....   | 5-69 |
| Figura 1.9 - Modo de Operación CFB.....  | 5-71 |
| Figura 1.10- Modo de Operación OFB.....  | 5-73 |
| Figura 1.11- Casos de encriptación múltiple.....   | 5-75 |
| Figura 1.12- Esquema Feistel.....  | 5-77 |
| Figura 1.13- La función Feistel (Función-F) de DES .....   | 5-78 |
| Figura 1.14- La generación de claves de DES .....  | 5-79 |
| Figura 1.15- Red Sustitución-Permutación (SP) .....  | 5-80 |
| Figura 1.16- El cilindro de Jefferson .....  | 6-86 |
| Figura 1.17- Máquina de rotores genérica.....  | 6-87 |