



**Maestría en Seguridad de Tecnologías de
Información
Controles Criptográficos de Seguridad
2023-3**

Profesor: Maestro Sánchez García Isaac Daniel

ENTREGABLE FINAL:
**“PROPUESTA DE PROYECTO EJECUTIVO DE
MÉTODOS DE CIFRADO Y PORTAFOLIO DE
EVIDENCIAS”**

Alumna: Kuhliger Martínez Martha Guadalupe

Número de Cuenta: 334011227

04 de junio del 2023

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS.....	3
ÍNDICE DE TABLAS	6
ÍNDICE DE ANEXOS.....	7
RESUMEN	8
ABSTRACT.....	9
CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA	10
Descripción de la realidad problemática	10
Formulación del problema.....	11
Objetivos de la propuesta.....	12
Objetivo general.....	12
Objetivos específicos	12
Alcance de la propuesta	12
CAPÍTULO II: MARCO TEÓRICO	13
Antecedentes de la investigación.....	13
Introducción al concepto de cifrado.....	13
Máquinas de cifrado	14
ENIGMA.....	14
SIGABA.....	15
TYPEX.....	15
CCM.....	15
PURPLE	16
Aplicación del cifrado a la industria	16
Introducción a la esteganografía.....	17
Esteganográfico.....	18
Aplicación de la esteganografía a la industria.....	27
Métodos de Cifrado Clásicos.....	28
Cifrado César.....	28
Cifrado de Sustitución Afines	34
Método Vigenère.....	36
Cifrado de Hill.....	39
Método de Alberti.....	52
Funciones de Cifrado Unidireccional	58

Definición del caso.....	58
Desarrollo de la solución al caso.....	60
Justificación de la solución.....	66
Conclusión del caso	67
CAPÍTULO II: DIAGNÓSTICO DEL ESTATUS DE LA EMPRESA	68
Misión.....	68
Visión.....	68
Historia.....	68
Organigrama.....	69
CAPÍTULO IV: PROPUESTA DE LA SOLUCIÓN	70
Diseño de la planeación de la propuesta.....	70
Justificación de la propuesta.....	71
Desarrollo del modelo criptográfico.....	73
Generar llaves en Kali Linux.....	73
Herramientas para método de cifrado	76
Recomendaciones	78
Fase de pruebas.....	79
CAPÍTULO V: CUESTIONARIO	80
CAPÍTULO VI: CONCLUSIONES.....	82
REFERENCIAS.....	84
ANEXOS.....	88
A. ESTÁNDAR DE CIFRADO DE DATOS (DES - DATA ENCRYPTION STANDARD)	88
B. TRIPLE DES.....	88
C. RIVEST SHAMIR ADLEMAN (RSA)	89

ÍNDICE DE FIGURAS

Figura 1. Elementos de la criptología.....	10
Figura 2. Flujo del correo electrónico.	11
Figura 3. Sistema Operativo Kali Linux.	18
Figura 4. Imagen original.....	18
Figura 5. Comando cd Desktop.....	19
Figura 6. Comando apt install steghide.....	19
Figura 7. Crear nuevo archivo en terminal Kali	20
Figura 8. Contenido del archivo mensaje.txt.	20
Figura 9. Comando para ocultar mensaje.	21
Figura 10. Solicitud de contraseña para imagen	21
Figura 11. Comparación de imagen original vs imagen con mensaje oculto	21
Figura 12. Comando para extraer mensaje.	22
Figura 13. Nuevo archivo con mensaje extraído de imagen.....	22
Figura 14. Mensaje extraído de imagen.....	22
Figura 15. Imagen original 02.	23
Figura 16. Directorio Downloads en Kali.	23
Figura 17. Comando para ejecutar herramienta imghide.py.....	23
Figura 18. Opción para cifrar en imghide.	24
Figura 19. Ruta de la imagen original.	24
Figura 20. Mensaje para ocultar.....	24
Figura 21. Contraseña del mensaje oculto	25
Figura 22. Ruta de la nueva imagen con texto cifrado.....	25
Figura 23 Opción para descifrar en imghide.....	26
Figura 24 Ruta de la imagen cifrada.	26
Figura 25. Contraseña para descifrar.	27
Figura 26. Mensaje descifrado.....	27
Figura 27. Cifrando mensaje con Cifrado César.	29
Figura 28. Identificar la palabra Hace.	30
Figura 29. Valores descifrados de la palabra Hace.	31
Figura 30. Proceso para identificar letras.....	32
Figura 31. Cuadro de Vigenère.....	37
Figura 32. Fórmula para cifrar letras con alfabeto cifrado.	38
Figura 33. Sumatoria de valor cifrado + llave cifrada en Excel.....	38
Figura 34. Aplicación del módulo 26.	38
Figura 35. Fórmula en Excel para cifrar.....	39
Figura 36. Plantilla en Excel para cifrar mensaje con Método Vigenère.....	39
Figura 37. División de bloques de cuatro caracteres.	41
Figura 38 Matrices generadas del mensaje.	41
Figura 39. Matriz cifrada.	42
Figura 40. Cálculo de la matriz del bloque 1.....	42
Figura 41. Valores descifrados del bloque 1.....	43
Figura 42. Cálculo de la matriz del bloque 2.....	43
Figura 43. Valores descifrados del bloque 2.....	44

Figura 44. Cálculo de la matriz del bloque 3.....	44
Figura 45. Valores descifrados del bloque 3.....	45
Figura 46.. Cálculo de la matriz del bloque 4.....	45
Figura 47. Valores descifrados del bloque 4.....	46
Figura 48. Matriz cifrada de Método Hill.	46
Figura 49. Matriz inversa por el Método Determinante.	47
Figura 50. Matriz traspuesta.....	48
Figura 51. Aplicación del módulo 27 a matriz.....	48
Figura 52. Cálculo y descifrado de la matriz del bloque 1.....	49
Figura 53. Cálculo y descifrado de la matriz del bloque 2.....	49
Figura 54. Cálculo y descifrado de la matriz del bloque 3.....	50
Figura 55. Cálculo y descifrado de la matriz del bloque 4.....	50
Figura 56. Cálculo y descifrado de la matriz del bloque 5.....	51
Figura 57. Cálculo y descifrado de la matriz del bloque 6.....	51
Figura 58. Cálculo y descifrado de la matriz del bloque 7.....	52
Figura 59. Ruleta de Alberti.	53
Figura 60. Primera vuelta con cinco saltos dos veces.....	54
Figura 61. Segunda vuelta con cinco saltos dos veces.....	54
Figura 62. Tercer vuelta con cinco saltos dos veces.	55
Figura 63. Cuarta vuelta con cinco saltos dos veces.....	55
Figura 64. Quinta vuelta con cinco saltos dos veces.	56
Figura 65. Sexta vuelta con cinco saltos dos veces.....	56
Figura 66. Séptima vuelta con cinco saltos dos veces.	57
Figura 67. Última vuelta con cinco saltos dos veces.....	57
Figura 68. Información adicional del caso.	59
Figura 69. Contenido del archivo USR02.....	60
Figura 70. Herramienta HashCalc.	60
Figura 71. Validar integridad del texto del archivo USR02 con HashCalc.	61
Figura 72 Validar integridad del texto alterado de USR02 con HashCalc.....	61
Figura 73. Validar integridad del archivo USR02 con HashCalc.	62
Figura 74. Texto del archivo USR02 alterado.....	62
Figura 75. Validar integridad del archivo alterado de USR02 con HashCalc.....	63
Figura 76. Validar integridad del archivo USR02 con SHA256 en Kali.....	63
Figura 77. Valor Hash en Kali.	63
Figura 78. Texto del archivo USR02 alterado en Kali.	64
Figura 79 Validar nuevamente la integridad del archivo USR02 con SHA256 en Kali.....	64
Figura 80. Valores Hash no coinciden.....	64
Figura 81. Código de proyecto en C# para validar integridad de texto.	65
Figura 82. Resultados de validar integridad en programa de C#.	66
Figura 83. Organigrama de la empresa MKuhligier S.A. DE C.V.	69
Figura 84. Diseño de la planeación de implementar métodos de cifrado.	70
Figura 85. Diagrama del RSA y DES implementados en el flujo de correo electrónico.	73
Figura 86. Comando para crear llaves de cifrado en Kali.	74
Figura 87. Ruta de las llaves cifradas.	74

Figura 88. Solicitud de contraseña para llaves de cifrado.	74
Figura 89. Creación de llaves de cifrado en Kali.	75
Figura 90. Llaves cifradas en Kali.	75
Figura 91. Llave de cifrado privada.	76
Figura 92. Llave de cifrado pública.	76
Figura 93. Herramienta GNUPG.	76
Figura 94. Método para cifrar con GNUPG.	77
Figura 95. Recomendaciones de métodos de cifrado.	78
Figura 96. Diagrama de Algoritmo DES.	88

ÍNDICE DE TABLAS

Tabla 1. Gráfica de Cifrado César.	28
Tabla 2. Alfabeto en español numerado.	29
Tabla 3. Alfabeto descifrado por método César.	31
Tabla 4. Alfabeto desplazado 10 lugares.	33
Tabla 5. Alfabeto por método de sustitución.	34
Tabla 6. Alfabeto en inglés numerado.	35
Tabla 7. Alfabeto descifrado por método de sustitución.	36
Tabla 8. Llave cifrada de Método Vigenère.	38
Tabla 9. Alfabeto en español numerado para Método Hill.	40
Tabla 10. Mensaje cifrado con Método Hill.	40
Tabla 11 Tabla 12. Alfabeto en español numerado del Método Hill.	47
Tabla 13. Catálogo de beneficios del algoritmo DES.	71
Tabla 14 Catálogo de beneficios del algoritmo RSA.	72
Tabla 15. Catálogo de características para método de cifrado.	78

ÍNDICE DE ANEXOS

A. ESTÁNDAR DE CIFRADO DE DATOS (DES - DATA ENCRYPTION STANDARD).....	88
B. TRIPLE DES.....	88
C. RIVEST SHAMIR ADLEMAN (RSA).....	89

RESUMEN

El presente trabajo consiste en implementar y reforzar los conocimientos y las tecnologías que se aprendieron en el curso de Controles Criptográficos de Seguridad para el diseño de una propuesta que proporcionará una mayor seguridad en el intercambio de información dentro de una organización para un caso de estudio de una empresa real, la cual se nombrará *MKuhliger S.A. DE C.V.* para este efecto.

El caso de estudio consistió en desarrollar una estrategia para implementar métodos de cifrado a los datos y documentos que la organización transfiere mediante el uso del correo electrónico para proteger la organización y guiarla adecuadamente, y así prevenir amenazas dañinas debido al mal manejo de la información y a la explotación de intrusos y ciberdelincuentes que vean como una oportunidad de acceder a información confidencial para sus propios intereses.

Se realizó una recopilación y análisis de información con respecto a los distintos métodos de cifrado que se han desarrollado desde su inicio, los algoritmos de cifrado, las herramientas que existen para facilitar el uso de los métodos de cifrado, su aplicación a la industria, las funciones de cifrado unidireccionales, problemas y explicaciones de cómo se realizan los métodos de cifrado y recomendaciones que se deben seguir para llevar a cabo una implementación exitosa y eficiente de los métodos de criptografía.

Con base en lo anterior, se desarrolló una propuesta para garantizar un mejor control de datos y gestionar la información, ejecutando métodos de cifrado y herramientas como OpenSSL y GNUPG, y generar llaves de cifrado para la organización *MKuhliger S.A. DE C.V.*

Se anexaron dentro del contenido del trabajo los entregables que se realizaron durante el curso, lo cuales son el ensayo sobre cifrado y esteganografía, la práctica de funciones de cifrado unidireccional el problemario de los métodos de cifrado clásicos, así como el cuestionario del curso.

De esta forma se podrá minimizar y mitigar los accesos a la información confidencial para proteger la integridad de los datos de la organización *MKuhliger S.A. DE C.V.* y de sus clientes, ante un ataque o amenaza, ya sea una acción voluntaria o involuntaria que puede surgir y causar un daño a la organización.

Por confidencialidad se ha modificado el nombre de la organización por *MKuhliger S.A. DE C.V.*, así como algunos detalles de la biografía de la organización.

ABSTRACT

The present work consists of implementing and reinforcing the knowledge and technologies learned in the Cryptographic Security Controls course for the design of a proposal that will provide greater security in the exchange of information within an organization for a case study of a real company, which will be named *MKuhliger S.A. DE C.V.* for this purpose.

The case study consisted of developing a strategy to implement encryption methods to the data and documents that the organization transfers through the use of email to protect the organization and guide it properly, and thus prevent harmful threats due to mishandling of information and exploitation of intruders and cybercriminals who see it as an opportunity to access confidential information for their own interests.

A compilation and analysis of information was carried out regarding the different encryption methods that have been developed since their inception, encryption algorithms, tools that exist to facilitate the use of encryption methods, their application to the industry, one-way encryption functions, problems and explanations of how encryption methods are performed and recommendations that should be followed to carry out a successful and efficient implementation of cryptography methods.

Based on the above, a proposal was developed to ensure better data control and information management, implementing encryption methods and tools such as OpenSSL and GNUPG, and generate encryption keys for the *MKuhliger S.A. DE C.V.* organization.

The deliverables that were made during the course, which are the essay on encryption and steganography, the practice of unidirectional encryption functions, the problem of classical encryption methods, as well as the course questionnaire, were annexed within the content of the work.

In this way it will be possible to minimize and mitigate access to confidential information to protect the integrity of the data of the organization *MKuhliger S.A. DE C.V.* and its customers, before an attack or threat, either a voluntary or involuntary action that may arise and cause damage to the organization.

For confidentiality reasons, the name of the organization has been changed to *MKuhliger S.A. DE C.V.*, as well as some details of the organization's biography.