Instituto Politécnico Nacional
Secretaría de Investigación y Posgrado
Dirección de Posgrado

SIP-30
2024

Formato para registro de Unidades de aprendizaje

I.- Datos de identificación de la Unidad de aprendizaje

Unidad académica:	CIDETEC			
Nombre del Programa académico:	Maestría en Tecnología de Cómputo			
	Grado Maestría		Orientación Profesional	
	Sesión de colegio donde se propuso:	Reunión ordinaria #8	Fecha de propuesta:	18/08/2025

Nombre de unidad de aprendizaje:	Cryptographic tools						
	Clave de la unidad de aprendizaje:	**16A7577**		Créditos:	5	*REP 2017*	
	Semanas por semestre	18	Horas a la semana:	4	Horas totales:	72	
Tipo de unidad de aprendizaje:	Obligatoria:	☐	Optativa:	☒	Observaciones:		
	Semestre:	1-3					

Área del conocimiento:	Ingeniería y Ciencias Fisico Matemáticas

Formato para registro de Unidades de aprendizaje

II. Aprendizajes que, al finalizar, el estudiantado deberá demostrar

Conocimientos	Habilidades y destrezas	Actitudes y valores
• Understanding of statistical metrics for evaluating cryptographic security. • Understanding of differential cryptanalysis, texture analysis, and cryptographic key security. • Interpretation of the NIST SP 800-22 statistical test suite for randomness evaluation.	• Apply statistical and probabilistic methods to assess the quality and robustness of encrypted information. • Implement and interpret experimental evaluations in cryptographic systems.	• Ethical responsibility in the application of cryptographic tools. • Evidence-based evaluation for objective decisions.

Resolución que aborda la propuesta con su enfoque disciplinar

Este rubro debe centrarse en los aspectos que resuelven o indagan la(s) disciplina(s) o tema(s) que se aborda(n), tome en cuenta que no se desea registrar aquí el estado del arte que guarda un conocimiento acumulado dentro de un área específica, sino la respuesta que se da con esta planeación didáctica ante una problemática definida.

Cryptographic tools address the need to evaluate the robustness of cryptographic algorithms through statistical and computational methods. The subject responds to the problem of determining whether encryption schemes provide sufficient resistance against statistical attacks and key vulnerabilities. The syllabus offers methodological tools to measure randomness, detect weaknesses, and quantify security. By integrating cryptography, statistics, and computation, the course provides to students a framework to critically validate encryption-security.

III. Proximidad formativa

Áreas multi, inter y transdisciplinarias:	*Líneas de Generación y Aplicación de Conocimiento:*	*Sectores sociales:*
Anote las disciplinas con las que se relacionan los temas de estudio de esta planeación. Tome en cuenta que su registro estará justificado si contempla información efectiva (y evidente) para el aprendizaje propuesto.	Se retoman del programa académico según corresponda.	Sectores sociales donde puedan promoverse los productos académicos que resultan del natural ejercicio formativo que se está planificando. Enuncie los sectores o grupos que consideres viables.

Formato para registro de Unidades de aprendizaje

• Applied Statistics • Information Security • Data Science • Ethics of Technology	• Tecnologías computacionales • Seguridad informática	• Information and Communication industry • Financial sector • Government and Defense

Estrategia de asociación:

Integre sintéticamente las consideraciones para delimitar cómo interactúa el estudiante con los sectores de la sociedad (previamente considerados) en función de la mediación de conocimientos que se pretende abordar y los aspectos que resuelve o indaga.

- Apply it in real contexts by analyzing datasets of encrypted information.
- Experimental evaluations based on international standards.
- Problem-oriented projects that replicate challenges faced by government, banks, and technology companies in evaluating encrypted information.

IV. Contenido temático (incluya el tiempo requerido si lo considera apropiado)

1.Statistical Analysis and Encryption Evaluation (26 hours)
1.1 Importance of Cryptographic Evaluation
1.2. Correlation Coefficient
1.3. Correlation of Adjacent Bytes
1.4. Correlation Between Plainbytes and Cipherbytes
1 Probabilistic Distributions in Cryptography
1.6. Maximum and Irregular Histogram Deviation
1.7. Entropy
1.8. Hypothesis Testing in Cryptographic Contexts
1.9. Interpretation of p-values in Security Evaluations
1.10. Chi-Square Goodness-of-Fit Test
1.11. Mean Square and Absolute Error
1.12. Peak Signal-to-Noise Ratio (PSNR)

2. Differential Cryptanalysis (8 hours)
2.1. Avalanche Effect and Bit Sensitivity
2.2. Number of Pixels Change Rate (NPCR)

Formato para registro de Unidades de aprendizaje

2.3. Unified Average Changing Intensity (UACI)
2.4. Similarity Parameter (SP)

3. Texture Analysis (8 hours)
3.1. Definition of Gray-Level Co-Occurrence Matrix
3.2. Homogeneity Metric
3.3. Contrast Measurement
3.4. Energy

4. Cryptographic Key Security (5 hours)
4.1. Key Permutation
4.2. Key Space Size
4.3. Key Sensitivity.

5. NIST SP 800-22 Statistical Test Suite (25 hours)
5.1. Frequency Tests
5.2. Runs and Longest Run of Ones Tests
5.3. Binary Matrix Rank Test
5.4. Discrete Fourier Transform Test
5.5. Non-overlapping and Overlapping Template Matching Tests
5.6. Maurer's Universal Statistical Test
5.7. Linear Complexity Test
5.8. Serial Test
5.9. Approximate Entropy Test
5.10. Cumulative Sums Test
5.11. Random Excursions and Random Excursions Variant Tests

V. Referencias

Documentales / electrónicas

1. Bassham, L., Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Leigh, S., Levenson, M., Vangel, M., Heckert, N., & Banks, D. (2010, September 16). A statistical test suite for random and pseudorandom number generators for cryptographic applications (NIST Special Publication 800-22rev1a). National Institute of Standards and Technology. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=906762
2. Alghamdi, Y., & Munir, A. (2024). Image encryption algorithms: A survey of design and evaluation metrics. Journal of Cybersecurity and Privacy, 4(1), 126–152. MDPI. https://doi.org/10.3390/jcp4010007

Formato para registro de Unidades de aprendizaje

3.	SaberiKamarposhti, M., Ghorbani, A., & Yadollahi, M. (2024). A comprehensive survey on image encryption: Taxonomy, challenges, and future directions. Chaos, Solitons & Fractals, 178, 114361. Elsevier. https://doi.org/10.1016/j.chaos.2023.114361
4.	Zia, U., McCartney, M., Scotney, B., Martinez, J., AbuTair, M., Memon, J., & Sajjad, A. (2022). Survey on image encryption techniques using chaotic maps in spatial, transform and spatiotemporal domains. International Journal of Information Security, 21(4), 917–935. Springer. https://doi.org/10.1007/s10207-021-00581-7
5.	Anusuya, K. V., & Navindran, N. (2022). Image security algorithms—Proposed methods and critical performance analysis for the best fit. In ICCCE 2021: Proceedings of the 4th International Conference on Communications and Cyber Physical Engineering (pp. 1135–1146). Springer. https://doi.org/10.1007/978-981-16-7985-8_118.
6.	Silva-García, V., Flores-Carapia, R., & González-Ramírez, M. (2023). Temas selectos de criptografía (1st ed., pp. 1–112). Alfaomega.
7.	Tamimi, A. A., Abdalla, A. M., & Abdallah, M. M. (2021). Utilizing quality measures in evaluating image encryption methods. In H. R. Arabnia, L. Deligiannidis, H. Shouno, F. G. Tinetti, & Q.-N. Tran (Eds.), Advances in computer vision and computational biology (pp. 271–278). Springer. https://doi.org/10.1007/978-3-030-71051-4_21

VI. Evaluación

The course is evaluated considering:

Homework 30%
Exam 30%
A final project 40%

VII. Créditos y responsivas

Responsabilidad	Nombre completo	Clave de nombramiento
Coordinador (Autor)	DR. VÍCTOR MANUEL SILVA GARCÍA	15504-EG-22/6
Participante (Coautor)	DR. ROLANDO FLORES CARAPIA	19112-EG-25
Participante (Coautor)	M. en T.C. MANUEL ALEJANDRO CARDONA LÓPEZ	