INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

PROGRAMA SINTÉTICO

UNIDAD ACADÉMICA: ESCUELA SUPERIOR DE CÓMPUTO, UNIDAD PROFESIONAL INTERDISCIPLINARIA DE INGENIERÍA, CAMPUS ZACATECAS	
PROGRAMA ACADÉMICO: Ingeniería en Sistemas Computacionales	
UNIDAD DE APRENDIZAJE: Introduction to cryptography	**SEMESTRE:** VI

PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Construye aplicaciones criptográficas con base en algoritmos, primitivas y servicios existentes de la criptografía de clave secreta y pública.

CONTENIDOS:

I. Fundamentos de criptografía
II. Criptografía de clave secreta
III. Integridad
IV. Criptografía de clave pública

ORIENTACIÓN DIDÁCTICA:

Métodos de enseñanza		Estrategias de aprendizaje	
a) Inductivo	x	a) Estudio de Casos	
b) Deductivo		b) Aprendizaje Basado en Problemas	
c) Analógico		c) Aprendizaje Orientado a Proyectos	x
d)Heurístico	x		

EVALUACIÓN Y ACREDITACIÓN:

Diagnóstica	x	Saberes Previamente Adquiridos	x
Solución de casos		Organizadores gráficos	x
Problemas resueltos		Problemarios	x
Reporte de proyectos	x	Exposiciones	x
Reportes de indagación	x	Otras evidencias a evaluar:	
Reportes de prácticas	x		
Evaluación escrita	x		

BIBLIOGRAFÍA BÁSICA:

Autor(es)	Año	Título del documento	Editorial/ ISBN
Menezes A., Oorschot, P. y Vanstone, S.	1996	Handbook of Applied Cryptography	CRC Press/ 978-0849385230
Para, C., Pelzl, J.	2014	Understanding Cryptography: a textbook for students and practitioners	Springer Verlag/ 978-3642446498
Stallings, W.	2017	Cryptography and network security: principles and practice	Pearson/ 978-1292158587
Stinson, D. R. y Paterson, M. B	2018	Cryptography: Theory and practice	CRC Press/ 978-1138197015
Trappe, W. y Washington, L.	2020	Introduction to Cryptography with coding Theory	Pearson/ 978-0134859064

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

PROGRAMA DE ESTUDIOS

UNIDAD ACADÉMICA: ESCUELA SUPERIOR DE CÓMPUTO, UNIDAD PROFESIONAL INTERDISCIPLINARIA DE INGENIERÍA, CAMPUS ZACATECAS		
PROGRAMA ACADÉMICO: Ingeniería en Sistemas Computacionales		
SEMESTRE: VI	**ÁREA DE FORMACIÓN:** Profesional	**MODALIDAD:** Escolarizada
TIPO DE UNIDAD DE APRENDIZAJE: Teórica-práctica/ Optativa		
VIGENTE A PARTIR DE: Agosto 2022	**CRÉDITOS:** **TEPIC:** 7.5	**SATCA:** 6.3

INTENCIÓN EDUCATIVA

La unidad de aprendizaje contribuye al perfil de egreso de la Ingeniería en Sistemas Computacionales al proveer técnicas y herramientas criptográficas para resolver problemas computacionales de acuerdo con estándares de calidad en seguridad al ofrecer confidencialidad, integridad, autenticación y no repudio en el intercambio de información. Asimismo, se desarrollan habilidades transversales como creatividad, resolución de problemas y trabajo en equipo.

Esta unidad de aprendizaje se relaciona de manera antecedente con Matemáticas discretas, Algoritmos y estructuras de datos, Análisis y diseño de algoritmos y Paradigmas de programación; y de forma consecuente con Selected Topics in Cryptography, Trabajo terminal I y Trabajo terminal II.

PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Construye aplicaciones criptográficas con base en algoritmos, primitivas y servicios existentes de la criptografía de clave secreta y pública.

TIEMPOS ASIGNADOS

HORAS TEORÍA/SEMANA: 3.0

HORAS PRÁCTICA/SEMANA: 1.5

HORAS TEORÍA/SEMESTRE: 54.0

HORAS PRÁCTICA/SEMESTRE: 27.0

HORAS APRENDIZAJE AUTÓNOMO: 24.0

HORAS TOTALES/SEMESTRE: 81.0

UNIDAD DE APRENDIZAJE REDISEÑADA POR: Academia de Ciencias de la Computación

REVISADA POR:

_____
M. en C. Iván Giovanny Mosso García

_____

Subdirección Académica ESCOM/UPIIZ

APROBADA POR:
Consejo Técnico Consultivo Escolar

_____
M. en C. Andrés Ortigoza Campos

_____
Dr. Fernando Flores Mejía
Presidente del CTCE de ESCOM/UPIIZ

dd/mm/aaaa

APROBADO POR: Comisión de Programas Académicos del Consejo General Consultivo del IPN.

dd/mm/aaaa

AUTORIZADO Y VALIDADO POR:

_____
Mtro. Mauricio Igor Jasso Zaranda
Director de Educación Superior

UNIDAD DE APRENDIZAJE: Introduction to cryptography **HOJA** 3 **DE** 7

UNIDAD TEMÁTICA I Fundamentos de criptografía	**CONTENIDO**	**HORAS CON DOCENTE**		**HRS AA**
		T	**P**	
UNIDAD DE COMPETENCIA Analiza los fundamentos e importancia de la criptografía, a partir de los cifradores clásicos y la aritmética en campos primos y binarios.	1.1 Fundamentos e importancia de criptografía 1.1.1 Notación 1.1.2 Clasificación 1.1.3 Ataques	1.5		
	1.2 Aritmética en campos primos 1.2.1 Suma, multiplicación, 1.2.2 Inverso aditivo y multiplicativo 1.2.3 Función de Euler	3.0	1.5	1.5
	1.3 Cifradores clásicos 1.3.1 Sustitución monoalfabética y polialfabética 1.3.2 Permutación	4.5	3.0	2.0
	1.4 Aritmética en campos binarios 1.4.1 Operaciones con polinomios de coeficientes en GF(2^8) 1.4.2 Suma, multiplicación y reducción binaria 1.4.3 Inversos multiplicativos	4.5		1.5
	Subtotal	13.5	4.5	5.0

UNIDAD TEMÁTICA II Criptografía de clave secreta	**CONTENIDO**	**HORAS CON DOCENTE**		**HRS AA**
		T	**P**	
UNIDAD DE COMPETENCIA Aplica los algoritmos de la criptografía de clave secreta con base en el funcionamiento de cifradores de flujo y de bloque.	2.1 Características de criptografía de clave secreta 2.1.2 Etapas del cifrado de clave secreta 2.1.3 Redes de sustitución- permutación	1.5		1.5
	2.2 Cifradores de bloque 2.2.1 DES 2.2.2 AES 2.2.4 Modos de operación	7.5	4.5	3.0
	2.3 Cifradores de flujo 2.3.1 Secreto perfecto 2.3.2 One time pad 2.3.3 Aplicaciones	3.0		1.5
	Subtotal	12.0	4.5	6.0

UNIDAD TEMÁTICA III Integridad	CONTENIDO	HORAS CON DOCENTE		HRS AA
		T	P	
UNIDAD DE COMPETENCIA Diseña soluciones a problemas de integridad de los datos a partir de las funciones hash y de los códigos de autenticación de mensaje.	3.1 Funciones hash criptográficas 3.1.1 Características y motivación 3.1.2 Colisiones débiles y fuertes 3.1.3 Problema del cumpleaños	4.5	1.5	2.0
	3.2 Códigos de Autenticación de Mensaje: MAC 3.2.1 Etapas 3.2.2 Construcción a partir de funciones hash y cifradores de bloque 3.2.3 Seguridad y aplicaciones de la MAC	3.0		1.0
	3.3 Soluciones a problemas de integridad de los datos con Hash y MAC 3.3.1 Integridad de los datos 3.3.2 Control de acceso 3.3.3 Autenticación de mensaje	1.5	3.0	1.0
	Subtotal	9.0	4.5	4.0

UNIDAD TEMÁTICA IV Criptografía de clave pública	CONTENIDO	HORAS CON DOCENTE		HRS AA
		T	P	
UNIDAD DE COMPETENCIA Crea soluciones a problemas de autenticación y no repudio a partir de los algoritmos de intercambio de claves Diffie Hellman, RSA y firma digital.	4.1 Características de criptografía de clave pública 4.1.1 Etapas del cifrado de clave pública 4.1.2 Funciones de un solo sentido: factorización en números primos y problema de logaritmo discreto	4.5	3.0	3.0
	4.2 Algoritmo de intercambio de claves Diffie-Hellman 4.2.1 Funcionamiento 4.2.2 Ataque del hombre de en medio	3.0 7.5	1.5 4.5	1.5 3.0
	4.3 RSA 4.3.1 Algoritmos de primalidad 4.3.2 RSA con teorema chino del residuo 4.3.3 RSA OAEP	 4.5	 4.5	 1.5
	4.4 Soluciones a problemas de autenticación y no repudio 4.4.1 Firma digital con RSA 4.4.3 Digital Signature Algorithm DSA			
	Subtotal	19.5	13.5	9.0

ESTRATEGIAS DE APRENDIZAJE	EVALUACIÓN DE LOS APRENDIZAJES
Estrategia de aprendizaje orientado a proyectos El alumno desarrollará las siguientes actividades: 1. Indagación previa de los temas a tratar en cada clase 2. Exposición de temas 3. Resolución de ejercicios teóricos de forma individual y en equipo 4. Realización de prácticas 5. Diseño e implementación de un proyecto para desarrollar una aplicación criptográfica en equipo.	Evaluación diagnóstica Portafolio de evidencias: 1. Organizadores gráficos 2. Diapositivas y guion para exposiciones 3. Ejercicios resueltos 4. Reporte de práctica 5. Reporte de proyecto y demostración del funcionamiento 6. Evaluación escrita

RELACIÓN DE PRÁCTICAS

PRÁCTICA No.	NOMBRE DE LA PRÁCTICA	UNIDADES TEMÁTICAS	LUGAR DE REALIZACIÓN
1	Criptoanálisis del cifrador Vigénere	I	Laboratorio De sistemas
2	Algoritmo extendido de Euclides	I	
3	Cifrador Hill y su criptoanálisis	I	
4	Cifrador de bloques con modos de operación	II	
5	Control de acceso: funciones hash	III	
6	Integridad: MAC	III	
7	Funciones de un solo sentido: factorización en primos y problema de logaritmo discreto	IV	
8	Intercambio de clave Diffie–Hellman	IV	
9	Firma digital: RSA, DSA	IV	
10	Criptografía híbrida	IV	
		TOTAL DE HORAS	27.0

Bibliografía

Tipo	Autor(es)	Año	Título del documento	Editorial/ISBN	Documento		
					Libro	Antología	Otros
B	Menezes, A. y Vanstone, S.	1996	Handbook of Applied Cryptography	CRC Press/ 9780849385230	X		
B	Para, C. y Pelzl, J.	2014	Understanding Cryptography: a textbook for students and practitioners	Springer Verlag/ 978-3642446498	X		
B	Stallings, W.	2017	Cryptography and network security: principles and practice	Pearson/ 978-1292158587	X		
B	Stinson, D. R., Paterson, M. B	2018	Cryptography: Theory and practice	CRC Press/978-1138197015	X		
B	Trappe, W. y Washington, L.	2020	Introduction to Cryptography with coding Theory	Pearson/978-0134859064	X		
C	Von zur Gathen, Joachim	2016	CryptoSchool	Springer Verlag/ 978-3662484241	X		
C	Knudsen, L. y Robshaw M.	2011	The block cipher companion	Springer Verlag/978-3642173431	X		
C	Kaufman, C, Perlman R., Speciner, M., Perlner, R.	2022	Network Security. Private communications in a public world	Addison-Wesley Proffesional/978-0136643609	X		

Recursos digitales

Autor, año, título y Dirección Electrónica	Texto	Simulador	Imagen	Tutorial	Video	Presentación	Diccionario	Otro
Cruise, B. (2022) Khan Academy: Computer science: Cryptorgraphy. https://es.khanacademy.org/computing/computer-science	X				X			
Cryptography. (2021). THE CRYPTPOGRAPHY OPEN SOURCE PROJECT. https://cryptography.io/en/latest/				X				
Nakov S. (2018). Practical Cryptography for Developers- Free Book. https://wizardforcel.gitbooks.io/practical-cryptography-for-developers-book/content/	X							
Crypto++. (2021). Crypto Library 8.6. https://cryptobook.nakov.com/crypto-libraries-for-developers								X
Bouncy Castle. (2022) (S/A). The legion of the Bouncy Castle. https://www.bouncycastle.org/documentation.html								X
IACR (2022). Cryptology ePrint Archive. https://eprint.iacr.org/								

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

PERFIL DOCENTE: Ingeniería o licenciatura en computación, con maestría en ciencias de la computación, matemáticas aplicadas o afín.

EXPERIENCIA PROFESIONAL	CONOCIMIENTOS	HABILIDADES DIDÁCTICAS	ACTITUDES
Dos años de experiencia en Criptografía Dos años en docencia a nivel superior Al menos un año de experiencia con el uso de bibliotecas criptográficas en lenguajes de alto nivel	Algoritmos criptográficos Teoría de grupos Teoría de números Complejidad algorítmica Lenguajes de programación de alto nivel Idioma Inglés Modelo Educativo Institucional	Coordinar grupos de aprendizaje Organizar equipos de aprendizaje Planificación de la enseñanza Manejo de estrategias didácticas centradas en el aprendizaje Manejo de TIC en la enseñanza y para el aprendizaje Comunicación multidireccional	Compromiso con la enseñanza Congruencia Disponibilidad al cambio Empatía Generosidad Honestidad Proactividad Respeto Responsabilidad Solidaridad Tolerancia Vocación de servicio Liderazgo

ELABORÓ

Dra. Nidia Asunción Cortez Duarte
Coordinadora

MHEP-TE Héctor Alejandro Acuña Cid
Coordinador

Dra. Sandra Díaz Santiago
Participante

Dr. Axel Ernesto Moreno Cervantes
Participante

M. en Ed. Karina Rodríguez Mejía
Participante

ISC. Efraín Arredondo Morales
Participante

REVISÓ

M. en C. Iván Giovanny Mosso García
Subdirección Académica
ESCOM

Subdirección Académica UPIIZ

AUTORIZÓ

M. en C. Andrés Ortigoza Campos
Director ESCOM

Dr. Fernando Flores Mejía
Director UPIIZ