INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

PROGRAMA SINTÉTICO

UNIDAD ACADÉMICA: ESCUELA SUPERIOR DE CÓMPUTO (ESCOM), UNIDAD PROFESIONAL INTERDISCIPLINARIA DE INGENIERÍA, CAMPUS ZACATECAS (UPIIZ)	
PROGRAMA ACADÉMICO: Ingeniería en Sistemas Computacionales	
UNIDAD DE APRENDIZAJE: Selected topics in cryptography	**SEMESTRE:** VII **PLAN DE ESTUDIOS:** 2020

PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Crea soluciones a problemas de seguridad de la información a partir de la criptografía basada en curvas elípticas, protocolos de seguridad y criptografía en dispositivos con recursos limitados.

CONTENIDOS:

I. Criptografía basada en curvas elípticas
II. Protocolos de seguridad que utilizan primitivas criptográficas
III. Criptografía para dispositivos con recursos limitados

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		**d)**	

EVALUACIÓN Y ACREDITACIÓN:

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

BIBLIOGRAFÍA BÁSICA:

Autor(es)	**Año**	**Título del documento**	**Editorial / ISBN**
Hankerson, D., Menezes A. J. y Vanstone, S.	2004	Guide to elliptic curve cryptography	Springer Verlag/ 978-0387952734
Kaufman, C., Perlman, R., Speciner, M. y Perlner, R.	2022	Network Security. Private communications in a public world	Addison-Wesley Proffesional/ 978-0136643609
Stinson, D. R. y Paterson M. B.	2018	Cryptography. Theory and Practice	CRC Press/ 1138197017
Van Oorschot, P.C.	2021	Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin	Springer Verlag/ 978-3030336486
Washington, L. C.	2008	Elliptic Curves. Number Theory and Cryptography	Chapman & Hall/CRC*I* 978-1420071467

INSTITUTO POLITÉCNICO NACIONAL

SECRETARÍA ACADÉMICA

DIRECCIÓN DE EDUCACIÓN SUPERIOR

PROGRAMA DE ESTUDIOS

UNIDAD ACADÉMICA: ESCUELA SUPERIOR DE CÓMPUTO (ESCOM), UNIDAD PROFESIONAL INTERDISCIPLINARIA DE INGENIERÍA, CAMPUS ZACATECAS (UPIIZ)		
PROGRAMA ACADÉMICO: Ingeniería en Sistemas Computacionales		
SEMESTRE: VII **PLAN DE ESTUDIOS:** 2020	**ÁREA DE FORMACIÓN:** Profesional	**MODALIDAD:** Escolarizada
TIPO DE UNIDAD DE APRENDIZAJE: Teórica- práctica/ Optativa		
VIGENTE A PARTIR DE: Enero 2023	**CRÉDITOS:** **TEPIC:** 7.5	**SATCA:** 6.3

INTENCIÓN EDUCATIVA

La unidad de aprendizaje contribuye al perfil de egreso de la Ingeniería en Sistemas Computacionales con el desarrollo de habilidades para diseñar algoritmos criptográficos eficientes para la solución de problemas de seguridad de la información, así como describir protocolos y esquemas de seguridad para garantizar el intercambio de información de manera confiable, a partir de componentes de hardware y software. Asimismo, fomenta las habilidades transversales como creatividad, trabajo en equipo, comunicación efectiva, y ética.

Esta unidad de aprendizaje se relaciona de manera antecedente con Introduction to cryptography; de manera lateral con Trabajo Terminal I; y de forma consecuente con Trabajo Terminal II.

PROPÓSITO DE LA UNIDAD DE APRENDIZAJE

Crea soluciones a problemas de seguridad de la información a partir de la criptografía basada en curvas elípticas, protocolos de seguridad y criptografía para dispositivos con recursos limitados.

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
Subdirector Académico ESCOM

_____
M. en C. Roberto Oswaldo Cruz Lejía
Subdirector Académico UPIIZ

APROBADA POR:
Consejo Técnico Consultivo Escolar

_____
M. en C. Andrés Ortigoza Campos
Presidente ESCOM
22/11/2022

_____
Dr. Fernando Flores Mejía
Presidente del CTCE de UPIIZ
27/06/2022

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

24/11/2022

AUTORIZADO Y VALIDADO POR:

_____
Mtro. Mauricio Igor Jasso Zaranda
Secretario Académico

UNIDAD TEMÁTICA I Criptografía basada en curvas elípticas	**CONTENIDO**	**HORAS CON DOCENTE**		**HRS AA**
		T	**P**	
UNIDAD DE COMPETENCIA Diseña aplicaciones criptográficas con base en la aritmética, los algoritmos criptográficos y los estándares para curvas elípticas.	1.1. Aritmética de curvas elípticas 1.1.1. Ecuación de Weierstrass 1.1.2. Ley de grupo 1.1.3. Curvas elípticas sobre campos finitos 1.2. Algoritmos criptográficos basados en curvas elípticas 1.2.1. Problema del logaritmo discreto en curvas elípticas 1.2.2. Intercambio seguro de claves: ECDH 1.2.3. Firma digital: ECDSA 1.3. Estándares para curvas elípticas 1.3.1. Curvas elípticas para intercambio de claves 1.3.2. Curvas elípticas para firma digital 1.3.3. Parámetros de seguridad para protocolos basados en curvas elípticas	7.0 8.0 3.0	4.5 3.0 1.5	3.0 3.0 2.0
	Subtotal	18.0	9.0	8.0

UNIDAD TEMÁTICA II Protocolos de seguridad que utilizan primitivas criptográficas	**CONTENIDO**	**HORAS CON DOCENTE**		**HRS AA**
		T	**P**	
UNIDAD DE COMPETENCIA Descubre escenarios de aplicación de los protocolos de seguridad, a partir de las primitivas criptográficas usadas en IPv4 e IPv6, protocolos de seguridad y aplicaciones de autenticación en internet.	2.1. Primitivas criptográficas usadas en IPv4 e IPv6 2.1.1. Primitivas usadas para brindar autenticación en IPSEC (ESP, AH): HMAC-SHA1-96, AES-XCBC-MAC-96, HMAC-MD5-96, AES-GCM, ChaCha20-Poly1305 2.1.2. Primitivas usadas para brindar confidencialidad en IPSEC (ESP): TripleDES-CBC, AES-CBC, AES-CTR 2.1.3. Mecanismos para la generación de claves 2.2. Criptografía aplicada en los protocolos de seguridad de Internet 2.2.1. Secure Email y S/MIME 2.2.2. Secure Sockets Layer (SSL) y Transport Layer Security (TLS) 2.2.3. HTTPS 2.2.4. Domain Keys Identified Mail (DKIM) 2.3. Aplicaciones de autenticación usadas en Internet 2.3.1. Kerberos 2.3.2. X509 2.3.3. Public-Key Infrastructure (PKI) 2.3.4. Gestión de identidad federada	6.0 6.0 6.0	3.0 3.0 3.0	3.0 2.5 2.5
	Subtotal	18.0	9.0	8.0

UNIDAD TEMÁTICA III Criptografía para dispositivos con recursos limitados	**CONTENIDO**	**HORAS CON DOCENTE**		**HRS AA**
		T	**P**	
UNIDAD DE COMPETENCIA Construye aplicaciones eficientes a partir de primitivas criptográficas en dispositivos con recursos limitados.	3.1. Características de la criptografía para dispositivos con recursos limitados 3.1.1. Dispositivos con recursos limitados 3.1.2. Métricas de desempeño en software 3.1.3. Métricas de desempeño en hardware	1.5	1.5	0.5
	3.2. Primitivas criptográficas 3.2.1. Cifradores de bloque 3.2.2. Cifrados de flujo 3.2.3. Códigos de Autenticación de Mensaje	6.0	3.0	3.0
	3.3. Diseño de aplicaciones criptográficas eficientes 3.3.1. Implementaciones en software 3.3.2. Implementaciones en hardware	10.5	4.5	4.5
	Subtotal	18.0	9.0	8.0

ESTRATEGIAS DE APRENDIZAJE	EVALUACIÓN DE LOS APRENDIZAJES
Estrategia de aprendizaje orientado a proyectos El alumno desarrollará las siguientes actividades: 1. Lectura de artículos académicos 2. Resolución de problemas teóricos de forma individual y en equipo 3. Exposiciones frente a grupo 4. Diseño e implementación de un proyecto para desarrollar una aplicación criptográfica. a. Planteamiento del problema de seguridad de la información b. Identificación de los servicios criptográficos y primitivas criptográficas a utilizar c. Diseño de la arquitectura de la aplicación a desarrollar d. Implementación de algoritmos criptográficos a partir de bibliotecas criptográficas e. Pruebas y presentación de resultados 5. Realización de prácticas	Evaluación diagnóstica Portafolio de evidencias: 1. Reportes de lectura y organizadores gráficos 2. Problemario resuelto 3. Presentación digital y guion de exposición 4. Reporte de proyecto 5. Reporte de prácticas 6. Evaluación escrita

RELACIÓN DE PRÁCTICAS

PRÁCTICA No.	NOMBRE DE LA PRÁCTICA	UNIDADES TEMÁTICAS	LUGAR DE REALIZACIÓN
1	Aritmética en curvas elípticas	I	Laboratorio
2	Dificultad del problema del logaritmo discreto en curvas elípticas.	I	
3	Protocolos criptográficos basados en curvas elípticas.	I	
4	Configuración de GnuPG para cifrar/autenticar correo electrónico	II	
5	Configuración de una VPN basada en IPSEC/SSL	II	
6	Cifradores de flujo para dispositivos con recursos limitados	III	
7	Cifradores de bloque para dispositivos con recursos limitados	III	
8	Aplicación de las primitivas criptográficas en dispositivos con recursos limitados	III	
		TOTAL DE HORAS:	27.0

Bibliografía

Tipo	Autor(es)	Año	Título del documento	Editorial/ ISBN	Documento		
					Libro	Antología	Otros
C	Cole, P.H. y Ranasinghe, D.C	2008	Networked RFID Systems and Lightweight Cryptography	Springer Verlag/ 0-13-277506-9	X		
B	Hankerson, D., Menezes, A. J. y Vanstone, S	2004	Guide to elliptic curve cryptography	Springer/ 978-0387952734	X		
B	Kaufman, C., Perlman, R., Speciner, M. y Perlner, R.	2022	Network Security. Private communications in a public world	Addison-Wesley Proffesional/ 978-0136643609			
C	Stallings, W. y Lawrie, B	2017	Computer Security. Principles and practice	Pearson/ 978-0134794105	X		
C	Stallings, W.	2017	Cryptography and Network Security. Principles and practice	Pearson/ 978-0134444284	X		
B	Stinson, D. R. y Paterson M. B.	2018	Cryptography. Theory and Practice	CRC Press/ 1138197017	X		
B	Van Oorschot, P.C.	2021	Computer Security and the Internet: Tools and Jewels from Malware to Bitcoin	Springer Verlag/ 978-3030336486	X		
B	Washington, L. C.	2008	Elliptic Curves. Number Theory and Cryptography	Chapman & Hall/CRC / 978-1420071467	X		
C	Wu, C.	2021	Internet of things security: Architectures and Security Measures	Springer Verlag/ 978-9811613715	X		

Recursos digitales

Autor, año, título y Dirección Electrónica	Texto	Simulador	Imagen	Tutorial	Video	Presentación	Diccionario	Otro
Cryptography. (2021). The cryptography 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							
Computer Security Resource Center. (2021). Lightweight cryptography. https://csrc.nist.gov/Projects/lightweight-cryptography/news								X
Computer Security Resource Center. (2021). Elliptic Curve Cryptography. https://csrc.nist.gov/Projects/elliptic-curve-cryptography/publications								X
Crypto++. (2021). Crypto Library 8.6. https://cryptobook.nakov.com/crypto-libraries-for-developers								X
Bouncy Castle. (S/A). The legion of the Bouncy Castle. https://www.bouncycastle.org/documentation.html								X
IACR (2022). Cryptology ePrint Archive. https://eprint.iacr.org/								X

INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE EDUCACIÓN SUPERIOR

PERFIL DOCENTE: Licenciatura en Computación o Ingeniería en Sistemas Computacionales con Maestría en Computación, Matemáticas o áreas afines.

EXPERIENCIA PROFESIONAL	CONOCIMIENTOS	HABILIDADES DIDÁCTICAS	ACTITUDES
Al menos dos años en docencia a nivel superior Al menos dos años en Criptografía Al menos un año en el uso de bibliotecas criptográficas	Criptografía Lenguajes de programación de alto nivel Teoría de grupos Teoría de números Del Modelo Educativo Institucional (MEI)	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 Honestidad Proactividad Respeto Responsabilidad Solidaridad Tolerancia Vocación de servicio Liderazgo

ELABORÓ **REVISÓ** **AUTORIZÓ**

Dra. Sandra Díaz Santiago
Coordinadora

Dra. Nidia Asunción Cortez Duarte
Participante

M. en C. Roberto Oswaldo Cruz Lejía
Subdirector Académico UPIIZ

M. en C. Andrés Ortigoza Campos
Director ESCOM

Dr. Axel Ernesto Moreno Cervantes
Participante

M. en C. Iván Giovanny Mosso García
Subdirector Académico ESCOM

Dr. Fernando Flores Mejía
Diector UPIIZ