Formato para registro de Unidades de aprendizaje 2021

INSTRUCTIVO para el correcto llenado del formato SIP-30

- El formato SIP-30 es un formato digital el cual puede ser completado con un procesador de texto y guardarse como archivo PDF para su envío.
- Adicionalmente será necesario anexar la solicitud firmada por el director de la Unidad Académica respectiva y el acuerdo de Colegio donde se avaló su registro; tenga listos los archivos al momento de ingresar su solicitud en el formulario en línea.
- El enlace de atención única para esta y otras gestiones es: https://forms.office.com/r/c8DLS6VBv1 (copie y pegue en un navegador web si el enlace no funciona)

- Tome en cuenta los criterios establecidos en el Reglamento de Estudios de Posgrado (REP 2017) para el llenado de este formato, a continuación se presentan algunas definiciones útiles:
  - *Número de semanas por semestre del programa:* Es el número de semanas lectivas efectivas al semestre, indicadas en el acuerdo de creación del programa académico o en alguna actualización posterior del programa. En caso de haber tenido una actualización en este sentido, la misma deberá haber sido presentada y avalada en reunión del Colegio de Profesores de la Unidad Académica, además de haber sido aprobada por la SIP. El rango de semanas lectivas al semestre es mínimo 15 y máximo 18.
  - *Tipo de horas:* Las unidades de aprendizaje, en cuanto a las horas asignadas, están clasificadas como: Teóricas, Prácticas y Teórico-prácticas. Estas denominaciones son excluyentes, es decir, las unidades de aprendizaje solo pueden ser de un solo tipo, no pueden tener horas combinadas.
  - *Número de horas – semana:* Es el número de horas asignadas para ser impartida la Unidad de Aprendizaje a la semana.
  - *Total de horas al semestre:* Es el número de horas totales a impartir de la Unidad de Aprendizaje al semestre. Se calcula multiplicando Número de semanas por número de horas-semana.
  - *Créditos* (Reglamento de Estudios de Posgrado 2017): FÓRMULA DE CÁLCULO: 16 hrs. = 1 crédito (horas totales / 16), no deben asignarse fracciones, los créditos deben redondearse a número entero.

- Para el registro de unidades de aprendizaje de modalidad no escolarizada o mixta incluya adicionalmente los campos marcados con el color azul
- En todos los campos existen comentarios en forma de globo que sirven de ayuda para el requisitado correspondiente, en caso de duda solicite apoyo del asesor didáctico de la UTEyCV de su Unidad Académica.

Instituto Politécnico Nacional

Secretaría Académica
Dirección de Educación Virtual

Secretaría de Investigación y Posgrado
Dirección de Posgrado

SIP-30

Formato para registro de Unidades de aprendizaje 2021

I.- Datos de identificación de la unidad de aprendizaje

Unidad académica:	CENTRO DE INVESTIGACIÓN EN COMPUTACIÓN								
Programa académico:	MAESTRÍA EN CIENCIAS EN INGENIERÍA DE CÓMPUTO								
		Doctorado				Orientación profesional			
	X	Maestría			X	Orientado a la investigación			
		Especialidad				Con la industria			
						Especialidad médica			
	Sesión de colegio donde se propuso:		10ª Ordinaria			Fecha de propuesta:		30 de octubre 2023	
Nombre de unidad de aprendizaje:	**Ingeniería Criptográfica**								
	Clave de la unidad de aprendizaje:					Créditos:	4	*REP 2017*	
	Semanas del semestre	18	Horas a la semana:	4		Horas totales:	72		
Tipo de unidad de aprendizaje:	Obligatoria:		Optativa:	X		Observaciones:			
	Semestre:								
	Teórica (%):		Práctica (%)			Teórico-prácticas (%):	100		
Área del conocimiento:	Ingeniería y Ciencias Fisicomatemáticas	X	Ciencias Sociales y Administrativas			Ciencias Medico Biológicas		Interdisciplinario	
Modalidad no escolarizada:	No escolarizada		Nombre de la Plataforma:						
	Mixta		Presencial (%):			En plataforma (%):			
Horas establecidas en el programa de estudios:	Presenciales (si procede) (horas x semana)					En plataforma (horas x semana):			

Formato para registro de Unidades de aprendizaje 2021

I. Aprendizajes que el estudiante deberá demostrar al finalizar

Conocimientos	Habilidades y destrezas	Actitudes y valores
• Técnicas de diseño para implementaciones de algoritmos de criptografía asimétrica. • Técnicas de diseño para implementaciones de algoritmos de criptografía simétrica. • Técnicas de diseño para implementaciones de algoritmos de resumen criptográfico. • Técnicas de diseño para implementaciones criptográficas resistentes ante ataques criptoanalíticos de canal lateral.	• Uso de técnicas de diseño para implementaciones criptográficas en hardware programable aplicables para cifrado asimétrico, cifrado simétrico, hash, así como para la generación de números pseudo-aleatorios. • Será capaz de valorar el uso de técnicas de protección ante posibles ataques a las implementaciones criptográficas.	• Será capaz de estimar el uso de controles de seguridad dentro del el diseño de una implementación criptográfica, acorde a los requerimientos de diseño. • Será capaz de analizar, discutir, justificar y recomendar decisiones de diseño, de manera rigurosa, asertiva, creativa, respetuosa, con apertura para la discusión y análisis. • Será capaz de elaborar argumentaciones sólidas en torno a los diseños desarrollados en materia de implementaciones criptográficas, promoviendo la presentación y defensa de sus ideas, manteniendo una apertura para la discusión.

Resolución que aborda la propuesta con su enfoque disciplinar

Esta unidad de aprendizaje brindará al estudiante los conocimientos teórico-prácticos necesarios para llevar a cabo la construcción o implementación de artefactos en hardware y/o en software que implementen la funcionalidad de los algoritmos criptográficos (descritos en la Unidad de Aprendizaje Introducción a la Criptografía), a fin de coadyuvar a la concretización de las ideas y propuestas de controles criptográficos, en el marco del diseño y desarrollo de esquemas, protocolos, arquitecturas y/o modelos de seguridad de la información. La unidad de aprendizaje está concebida para promover el aprendizaje del uso de las técnicas referidas a través de la realización de un conjunto de experiencias de desarrollo de proyectos de construcción a través de hardware programable y/o programación de software embebido.

Formato para registro de Unidades de aprendizaje 2021

II. Proximidad formativa

Áreas multi, inter y transdisciplinarias	Líneas de Generación y Aplicación de Conocimiento	Sectores sociales
• Introducción a la criptografía • Fundamentos matemáticos de la criptografía. • Lenguajes de programación de hardware • Programación de microcontroladores • Protocolos criptográficos • Arquitectura de computadoras • Internet de las cosas	• Ciencias y Tecnologías de la Información	• Los conocimientos, habilidades y destrezas adquiridos mediante esta unidad de aprendizaje permitirán al estudiante impactar de forma positiva en el sector industrial y de servicios, a través las acciones de diseño y construcción de artefactos para la protección de la seguridad de la información en las organizaciones.

Estrategia de asociación:

El estudiante desarrollará a lo largo del curso un conjunto de artefactos, los cuales le permitirán abordar desde un enfoque incremental el diseño de una solución tecnológica encaminada a resolver un problema objetivo, para lo cual involucrará requerimientos de diseño, limitantes del tecnológicas, así como restricciones asociadas al entorno de aplicación, las cuales servirán como guía para la toma de decisiones de diseño durante todo el curso, replicando así las condiciones del abordaje a una necesidad similar en un entorno real de aplicación.

III Metodología de enseñanza – aprendizaje

Descripción

Evidencias como proceso de aprendizaje	Evidencias integradoras (resultados que contribuyen al curriculum)	Ponderación

Formato para registro de Unidades de aprendizaje 2021

IV. Descripción de la participación esperada en el estudiante

Receptiva	Resolutiva	Autónoma	Estratégica

V. Secuencia programática

Contenido temático

I. Implementación de aritmética de campo finitos primos (18 horas)
- a. Adición, Multiplicación y reducción modular en Zn
- b. Construcciones para RSA
- c. Construcciones para Diffie Hellman / ElGamal

II. Implementación de aritmética de campos finitos binarios (18 horas)
- a. Adición, Multiplicación y reducción en campos binarios
- b. Multiplicación y reducción en extensiones de campos binarios
- c. Exponenciación
- d. Inversos Multiplicativos

III. Implementación de cifradores simétricos (16 horas)
- a. Gestión de bloques y relleno
- b. Cajas de substitución
- c. Rotación y translación
- d. Generación de subllaves

IV. Implementación de Funciones hash (12 horas)
- a. Construcción general de Merkle Damgard
- b. Familia MD-SHA
- c. Algoritmo SHA-3 y Keccak

V. Técnicas para prevención de ataques de canal lateral (8 horas)
- a. Análisis de tiempos
- b. Análisis de consumo de energía
- c. Análisis diferencial de consumo de energía
- d. Diseño de contramedidas
- e. Consideraciones de arquitectura

No.	Tema	Objetivo de aprendizaje / competencia específica	Tiempo/Horas/Semanas

Actividad(es):	No. Nombre de la actividad: Descripción de la actividad:	Tipo de interacción(es):	
		Referencias (s):	
Evidencia(s):			

Tipo de interacción: ID–Instrucción directa, TC–Trabajo colaborativo, AC–Análisis en campo, RP–Reflexión personal, PE–Presentación expositiva

Indicar solo el número de las *Referencias* indizadas en la sección VII de este documento.

Nota: Replique esta sección las veces que sea necesario para cubrir toda la secuencia programática

Formato para registro de Unidades de aprendizaje 2021

VI. Habilitadores tecnológicos

	Disposiciones	Especificaciones / descripción de efectos
	Conectividad	
	Habilidades digitales	
	Interoperabilidad	
	Datos abiertos	
	Big Data	
	Machine Learning	
	Simulación	
	Realidad aumentada	
	Otro…	

VII. Referencias

Conferencias magistrales	Notas complementarias

Documentales / electrónicas

1. Cryptographic Engineering, Çetin Kaya Koç Ed., Springer, 2009.
2. Cryptographic Algorithms on Reconfigurable Hardware, Rodriguez-Henriquez, Saqib, A. Diaz-Perez, Çetin Kaya Koç, Springer, 2006.
3. Cryptography Engineering: Design Principles and Practical Applications, Ferguson, Schneier, Khono, Wiley, 2010.

Formato para registro de Unidades de aprendizaje 2021

4. Reconfigurable Cryptographic Processor, Liu, Wang, Wei, Springer, 2018.
5. Handbook of Applied Cryptography, Menezes, Oorschot, Vanstone, CRC Press, 1996.
6. Elliptic Curves: Number Theory and Cryptography, Washington, Chapman and Hall/CRC, 2008.
7. Guide to Elliptic Curve Cryptography, Hankerson, Menezes, Vanstone, Springer, 2010.
8. Handbook of Elliptic and Hyperelliptic Curve Cryptography (Discrete Mathematics and Its Applications), Chapman and Hall/CRC, 2005.

VIII. Créditos y responsivas

	Responsabilidad	Nombre completo	Clave de nombramiento /No. de empleado
	Coordinador (Autor)	Dr. Moisés Salinas Rosales	15766-EF-22
	Participante (Coautor)	Dra. Gina Gallegos García	16939-EF-22
	Participante (Coautor)	M. en C. Osvaldo Espinosa Sosa	16370-EI-22
	Tecnólogo educativo / Comunicólogo		
	Corrector de estilo		
	Programador multimedia / Diseñador gráfico		
Otro…			

VERIFICACIÓN GENERAL DE LA PLANEACIÓN DIDÁCTICA REVISIÓN DE LA PLANEACIÓN DIDÁCTICA (VIABILIDAD)

Instituto Politécnico Nacional

Secretaría Académica
Dirección de Educación Virtual

Secretaría de Investigación y Posgrado
Dirección de Posgrado

SIP-30

Formato para registro de Unidades de aprendizaje 2021

Por la División de Operación y Promoción al Posgrado de la SIP	Por la Subdirección de Diseño y Desarrollo de la DEV
Nombre_____	Nombre_____
FIRMA_____	FIRMA_____

VERIFICACIÓN PARA SU PUESTA EN OPERACIÓN	REVISIÓN TÉCNICO-PEDAGÓGICA PARA LA MODALIDAD
Por la Dirección de Posgrado	Por la Dirección para la Educación Virtual
Nombre_____	Nombre_____
FIRMA_____	FIRMA_____
SELLO DE VALIDACIÓN	