Universidad Nacional de Ingeniería (UNI)
Escuela Profesional de
Ciberseguridad
Sílabo 2024-II

1. CURSO

CY311. Criptografía Avanzada (Obligatorio)

2. INFORMACIÓN GENERAL

2.1 Curso	:	CY311. Criptografía Avanzada
2.2 Semestre	:	10^{mo} Semestre.
2.3 Créditos	:	3
2.4 horas	:	2 HT; 2 HP;
2.5 Duración del periodo	:	16 semanas
2.6 Condición	:	Obligatorio
2.7 Modalidad de aprendizaje	:	Presencial
2.8 Prerrequisitos	:	CY211. Seguridad de Datos. (8^{vo} Sem)

3. PROFESORES

Atención previa coordinación con el profesor

4. INTRODUCCIÓN AL CURSO

Este curso profundiza en la criptografía, abordando conceptos avanzados y su aplicación en la seguridad de la información. Se analizan algoritmos de cifrado simétrico y asimétrico, criptoanálisis, firmas digitales y protocolos de seguridad, capacitando a los estudiantes para diseñar e implementar soluciones criptográficas robustas.

5. OBJETIVOS

- Comprender y aplicar algoritmos de cifrado simétrico y asimétrico avanzados.
- Analizar la seguridad de los sistemas criptográficos y realizar criptoanálisis.
- Diseñar e implementar protocolos de seguridad utilizando criptografía avanzada.

6. RESULTADOS DEL ESTUDIANTE

1) Analizar un problema computacional complejo y aplicar los principios computacionales y otras disciplinas relevantes para identificar soluciones. (Assessment)

6) Aplicar principios y prácticas de seguridad para mantener las operaciones en presencia de riesgos y amenazas. (Assessment)

7. TEMAS

Unidad 1: Criptografía (16 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Conceptos básicos – Cifrado/descifrado, autenticación del remitente, integridad de datos, no repudio – Clasificación de ataques (solo texto cifrado, texto sin formato conocido, texto sin formato elegido, texto cifrado elegido) – Clave secreta (simétrica), criptografía y criptografía de clave pública (asimétrica) – Seguridad teórica de la información (libreta de un solo uso, teorema de Shannon) – Seguridad computacional • Conceptos avanzados – Protocolos avanzados ∗ Pruebas y protocolos de conocimiento cero ∗ Intercambio de secretos ∗ Compromiso ∗ Transferencia ajena ∗ Computación multipartita segura – Desarrollos recientes avanzados: cifrado totalmente homomórfico, ofuscación, criptografía cuántica y esquema KLJN • Antecedentes matemáticos – Aritmética modular – Teoremas de Fermat y Euler – Raíces primitivas, problema de registros discretos – Prueba de primalidad, factorización de números enteros grandes – Curvas elípticas, celosías y problemas de celosías duras. – Álgebra abstracta, campos finitos. – Teoría de la información. • Cifrados históricos – Cifrado por desplazamiento, cifrado afín, cifrado por sustitución, cifrado Vigenere, ROT-13 – Cifrado Hill, máquina Enigma y otros. • Cifrados simétricos (clave privada) – Cifrados de bloque B y cifrados de flujo (permutaciones pseudoaleatorias, generadores pseudoaleatorios) – Redes Feistel, Estándar de cifrado de datos (DES) – Estándar de cifrado avanzado (AES) – Modos de funcionamiento de cifrados en bloque – Ataque diferencial, ataque lineal.	• Describa el propósito de la criptografía y enumere las formas en que se utiliza en las comunicaciones de datos [Usar] • Describa los siguientes términos: cifrado, criptoanálisis, algoritmo criptográfico y criptología, y describa los dos métodos básicos (cifrados) para transformar texto sin formato en texto cifrado [Usar] • Explique cómo la infraestructura de clave pública admite la firma y el cifrado digitales y analice las limitaciones/vulnerabilidades [Usar] • Discutir los peligros de inventar sus propios métodos criptográficos [Usar] • Describir qué protocolos, herramientas y técnicas criptográficas son apropiados para una situación determinada [Usar] • Explicar los objetivos de la seguridad de datos de un extremo a otro [Usar]

Unidad 2: Criptoanálisis (16 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Ataques clásicos – Ataque de fuerza bruta – Ataques basados en frecuencia – Ataques a la máquina Enigma – Ataque de paradoja del cumpleaños • Ataques de canal lateral – Ataques de tiempo – Ataques de consumo de energía – Análisis de fallas diferenciales • Ataques contra cifrados de clave privada – Ataque diferencial – Ataque lineal – Ataque de encuentro en el medio • Ataques contra cifrados de clave pública – Este tema incluye algoritmos de factorización: ∗ Métodos p-1 y rho de Pollard ∗ Tamiz cuadrático ∗ Tamiz de campos numéricos • Algoritmos para resolver el problema de los registros discretos – Pohlig-Hellman – Paso de bebé/Paso gigante – El método rho de Pollard • Ataques a RSA – Módulo compartido – Pequeño exponente público – Factores primos parcialmente expuestos	• Describir las diversas técnicas para el borrado de datos [Usar]
Lecturas : [**Boneh2020**]	

Unidad 3: Protocolos de comunicación seguros (16 horas)	
Resultados esperados: 1,6	
Temas	**Objetivos de Aprendizaje (*Learning Outcomes*)**
• Protocolos de capa de aplicación y transporte – HTTP – HTTPS – SSH – SSL/TLS • Ataques en TLS – Ataques de degradación – falsificación de certificados – Implicaciones de los certificados raíz robados – Transparencia del certificado • Internet/capa de red – IPsec – VPN • Protocolos de preservación de la privacidad – Mixnet – Tor – Mensajes extraoficiales – Signal • Capa de enlace de datos – L2TP – PPP – RADIUS	• Describir las diversas técnicas para el borrado de datos [Usar] • Explicar los objetivos de la seguridad de datos de un extremo a otro [Usar]
Lecturas : [**Aumasson2017**]	

8. PLAN DE TRABAJO

8.1 Metodología

Se fomenta la participación individual y en equipo para exponer sus ideas, motivándolos con puntos adicionales en las diferentes etapas de la evaluación del curso.

8.2 Sesiones Teóricas

Las sesiones de teoría se llevan a cabo en clases magistrales donde se realizarán actividades que propicien un aprendizaje activo, con dinámicas que permitan a los estudiantes interiorizar los conceptos.

8.3 Sesiones Prácticas

Las sesiones prácticas se llevan en clase donde se desarrollan una serie de ejercicios y/o conceptos prácticos mediante planteamiento de problemas, la resolución de problemas, ejercicios puntuales y/o en contextos aplicativos.

9. SISTEMA DE EVALUACIÓN

********* EVALUATION MISSING ********

10. BIBLIOGRAFÍA BÁSICA