National University of Engineering (UNI)
School of Cybersecurity
Syllabus 2024-II

1. COURSE

CY311. Advanced Cryptography (Mandatory)

2. GENERAL INFORMATION

2.1 Course	:	CY311. Advanced Cryptography
2.2 Semester	:	10^{th} Semester.
2.3 Credits	:	3
2.4 Horas	:	2 HT; 2 HP;
2.5 Duration of the period	:	16 weeks
2.6 Type of course	:	Mandatory
2.7 Learning modality	:	Face to face
2.8 Prerrequisites	:	CY211. Data Security. (8^{th} Sem)

3. PROFESSORS

Meetings after coordination with the professor

4. INTRODUCTION TO THE COURSE

This course delves into cryptography, covering advanced concepts and their application in information security. Symmetric and asymmetric encryption algorithms, cryptanalysis, digital signatures, and security protocols are analyzed, enabling students to design and implement robust cryptographic solutions.

5. GOALS

- Understand and apply advanced symmetric and asymmetric encryption algorithms.
- Analyze the security of cryptographic systems and perform cryptanalysis.
- Design and implement security protocols using advanced cryptography.

6. COMPETENCES

1) Analyze a complex computing problem and apply principles of computing and other relevant disciplines to identify solutions. (Assessment)

6) Apply security principles and practices to maintain operations in the presence of risks and threats. (Assessment)

7. TOPICS

Unit 1: Criptografía (16 hours)	
Competences Expected: 1,6	
Topics	**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]

Unit 2: Criptoanálisis (16 hours)

Competences Expected: 1,6

Topics	**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]

Readings : [**Boneh2020**]

Unit 3: Protocolos de comunicación seguros (16 hours)	
Competences Expected: 1,6	
Topics	**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]
Readings : [**Aumasson2017**]	

8. WORKPLAN

8.1 Methodology

Individual and team participation is encouraged to present their ideas, motivating them with additional points in the different stages of the course evaluation.

8.2 Theory Sessions

The theory sessions are held in master classes with activities including active learning and roleplay to allow students to internalize the concepts.

8.3 Practical Sessions

The practical sessions are held in class where a series of exercises and/or practical concepts are developed through problem solving, problem solving, specific exercises and/or in application contexts.

9. EVALUATION SYSTEM

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

10. BASIC BIBLIOGRAPHY