1. Identificación de la asignatura

División: Ingenierías

Departamento: Ingeniería de Sistemas.

Nombre de la asignatura: Criptografía

Código de la asignatura: ELP 8011

Nivel de la asignatura (Pregrado, Postgrado): Pregrado.

Requisitos (Código y nombre de la asignatura):

Número de créditos de la asignatura: 3

No. de horas teóricas por semana: 3

No. de horas prácticas por semana: 0

No. de horas trabajo independiente por semana: 6

Número de semanas: 16

Idioma de la asignatura: Español.
(Español, Inglés, Alemán, francés, otros)

Modalidad de la asignatura: Presencial.
(Presencial, Virtual, Híbrido, otros)

Nombre del profesor: Eduardo David Angulo Madrid

NRC: 1835

Contacto del profesor: edangulo@uninorte.edu.co

Horario de atención (si aplica): Con cita.

2. Descripción de la asignatura.

Esta asignatura presenta una introducción a criptografía. En principio se estudian los servicios de seguridad provistos por criptografía, y algoritmos históricos. Luego estudiamos el servicio de confidencialidad, particularmente estudiamos esquemas de cifrado simétricos, i.e. esquemas de cifrados simétrico de flujo y de bloque. Posteriormente, estudiamos esquemas de cifrado asimétricos. Luego estudiamos otro servicio provisto por criptografía, integridad de los datos, e introducimos nuevas primitivas criptográficas para ello. Particularmente, se estudia funciones hash criptográficas, código de autenticación de mensajes y firmas digitales. Luego estudiamos métodos de autenticación e intercambio de llaves, y finalmente estudiaremos aplicaciones criptográficas en el mundo real.

3. Justificación

Los más recientes avances en tecnologías han cambiado drásticamente la manera como las compañías hacen negocios. Avances tales como la evolución móvil, “big data” y e-commerce han hecho de la información el activo más importante en cada compañía. Por tal razón, proteger y asegurar la información debe ser un proceso clave para cualquier compañía. Las tecnologías y herramientas provistas por la criptografía son las más adecuadas para que una organización pueda asegurar y proteger sus procesos productivos.

4. Objetivo general de la asignatura.

Conocer sobre el funcionamiento interno de sistemas criptográficos y como usarlos correctamente en algunas aplicaciones reales.

Objetivos específicos:

OB1. Explicar los conceptos relacionados con los servicios de seguridad provistos por criptografía.

OB2. Explicar el concepto de un cifrador simétrico, cifradores en flujo y en bloque. Además, conocer los cifradores en bloque más populares.

OB3. Explicar el concepto de un cifrador asimétrico, basados en factorización y basados en el logaritmo discreto.

OB4. Explicar los conceptos fundamentales relacionados con integridad de los datos, y las primitivas criptográficas para proveerlo.

OB5. Explicar los conceptos fundamentales relacionados con autenticación, y las estrategias criptográficas para proveerlo.

OB6. Conocer las implementaciones populares de algoritmos criptográficos.

5. Resultados de Aprendizaje.

5.1. Course Outcomes

CO1. Explicar los conceptos relacionados con los servicios de seguridad provistos por criptografía.

CO2. Explicar el concepto de cifrado simétrico, cifradores en flujo y en bloque. Además, aprender a detalle alguno de los esquemas de cifrado en bloque y sus implementaciones más populares.

CO3. Explicar el concepto de cifrado asimétrico y las construcciones criptográficas más populares. Además, familiarizarse con su uso e implementación en aplicaciones reales.

CO4. Explicar los conceptos fundamentales relacionados con integridad de los datos, y las primitivas criptográficas para proveer integridad de los datos, tales como funciones hash criptográficas, códigos de autenticación de mensajes, y firma digital. Además, familiarizarse con su uso e implementación en aplicaciones reales.

CO5. Explicar los conceptos fundamentales relacionados con protocolos de autenticación e intercambio de llaves, y familiarizarse con construcciones y protocolos criptográficos populares.

5.2. Student Outcomes

Esta asignatura contribuye con el logro de los siguientes Student Outcomes, del modelo ABET:

SO7. Habilidad para adquirir y aplicar nuevo conocimiento según sea necesario, utilizando estrategias de aprendizaje apropiado.

6. Temas de la asignatura.

Tema	Subtemas	Número de Horas
Introducción	Servicios de seguridad provistos por criptografía	3
Herramientas Criptográficas	**Confidencialidad de los datos** Fundamentos de esquemas de cifrado simétrico Esquemas de cifrado históricos Esquemas criptográficos simétricos de flujo y de bloque • Salsa20 • Chacha20 • AES Modos de operación para esquemas criptográficos de bloque Esquemas criptográficos asimétricos • Basados en factorización • Basado en el logaritmo discreto	24
	Integridad de los datos Funciones hash criptográficas Códigos de autenticación de mensajes Esquemas de firmas digitales	9
Protocolos Criptográficos	Protocolos para identificación y acceso Protocolos de intercambio de llaves autenticado Comunicaciones anónimas: Protocolo TOR	12

7. Evaluación

Evaluaciones	Porcentaje	Temas	Semana
Parcial 1*	25%	Esquemas criptográficos simétricos y modos de operación	6
Parcial 2 *	25%	Esquemas criptográficos asimétricos e integridad de los datos	10
Proyecto	30%	Incluye todos los temas	2 a 16
Examen Final	20%	Incluye todos los temas	Semana de finales

(*) Componentes que corresponden al 40%.

8. Assessment

Salidas del curso (SOs) → ↓ Competencias adquiridas		CO1	CO2	CO3	CO4	CO5	Salidas del alumno SOs
Dominio Cognitivo 70%	Conocimiento	PAR1		PAR2		E.FINAL	
	Comprensión		PAR1	PAR2		E.FINAL	
	Análisis		PAR1	PAR2			
	Evaluación				PAR2	E.FINAL	
I+D 30%				E1	E2	E3	7

No se tolerará el **plagio** o la **copia**. Sin excepción, en caso de darse uno de estos casos, a los estudiantes involucrados se les iniciará proceso disciplinario, y se actuará conforme al Reglamento de Estudiantes de la Universidad del Norte. El plagio incluye usar contenidos sin la debida referencia, de manera literal o con mínimos cambios que no alteren el espíritu del texto. Adicionalmente, el estudiante debe tener presente que todos los exámenes, informes, trabajos, presentaciones, laboratorios y cualquier otro producto a evaluar debe:

- Ser realizado de forma individual, excepto, en aquellos casos en que el profesor lo autorice por escrito y sin ninguna clase de participación de terceros.
- Ser realizado en el periodo estipulado por el docente.
- Debe referenciar en el código fuente las librerías o algoritmos de terceros que hayan sido utilizados. Dar crédito a los autores de las ideas, conceptos teorías, datos en los que se basó el estudiante para realizar su trabajo.
- Debe enviarse por el medio definido por el docente. Si el trabajo debe ser enviado por catálogo web, sólo se recibirá por ese medio, y no por medios alternativos. En caso de no utilizar los medios establecidos para el desarrollo del curso, se asumirá que el trabajo no fue enviado.

9. Bibliografía

[1] *Jeffrey Hoffstein, Jill Pipher, and J. H. Silverman. 2014. An Introduction to Mathematical Cryptography (2nd ed.). Springer Publishing Company, Incorporated.*

[2] *Alfred J. Menezes, Scott A. Vanstone, and Paul C. Van Oorschot. 1996. Handbook of Applied Cryptography (1st ed.). CRC Press, Inc., Boca Raton, FL, USA.*

[3] *Keith Martin. 2017. Everyday Cryptography: Fundamental Principles and Applications (2 ed.). Oxford University Press.*

[4] *Christof Paar and Jan Pelzl. 2009. Understanding Cryptography: A Textbook for Students and Practitioners (1st ed.). Springer Publishing Company, Incorporated.*

[5] *Nigel P. Smart. 2015. Cryptography Made Simple (1st ed.). Springer Publishing Company, Incorporated.*

[6] *Ross J. Anderson. 2020. Security Engineering: A Guide to Building Dependable Distributed Systems (3 ed.). Wiley Publishing.*

[7] *D. Boneh and Victor Shoup. A Graduate Course in Applied Cryptography. Available at https://toc.cryptobook.us/*