Aprobado por resolución N°113 del CFI de fecha 04.07.2017

FACULTAD DE INGENIERIA

UNIVERSIDAD DE LA REPÚBLICA URUGUAY

Programa de Criptografía

1. NOMBRE DE LA UNIDAD CURRICULAR

Criptografía.

2. CRÉDITOS

10 (diez)

3. OBJETIVOS DE LA UNIDAD CURRICULAR

Dar un curso de criptografía orientado a estudiantes de ingeniería. En estsentido se espera balancear tanto aspectos teóricos como aspectos algorítimicos y aspectos orientados al uso de la criptografía en la práctica profesional. Se estudiarán también diversos aspectos relacionados con los estándares NIST. De haber tiempo, se espera completar con algunos datos de la historia de la criptografía que ayuden a ilustrar diversos conceptos.

Se espera que quienes tomen el curso, terminen teniendo no sólo fundamentos básicos sobre la criptografía, sino que también ideas claras sobre su uso en la profesión.

4. METODOLOGÍA DE ENSEÑANZA

El curso tiene una visión integral teórico-práctico. En este sentido, los conceptos dados en clase van a estar ilustrados con una gran cantidad de ejemplos y de ejercicios que se irán realizando tanto en clase como en ejercicios obligatorios.

Los ejercicios obligatorios se realizarán en cuatro entregas y son individuales. Varias clases teórico-prácticas van a estar dedicadas a discutir estos ejercicios obligatorios. Van a haber además dos laboratorios con entrega de informes, que también van a ser considerados para fijar la nota final del curso.

Las clases son interactivas con mucha participación estudiantil y con una dinámica consistente en dejar material de lectura para discutir en la clase siguiente. En las clases se va a hacer énfasis en aspectos fundamentales de cada tema que no están presentes en los libros, pero que van a ayudar sustancialmente a entender los temas cuando los estudiantes

lean el material. Por tal motivo la asistencia a clase es obligatoria en el entendido de que da mucho valor agregado para el aprovechamiento del curso.

Horas clases teórico-prácticas:	60 hs.
Horas de estudio para clases:	30 hs.
Horas trabajo obligatorio y laboratorio:	60 hs.
Total:	150 hs.

5. TEMARIO

1. Introducción y motivación histórica de la criptografía.
2. Criptosistemas básicos de clave privada. AES. Diffie-Hellman y acuerdos de Claves.
3. RSA y el problema de factorización. Análisis de seguridad de RSA. Test de Primalidad y generación de números primos seguros. Teorema Chino del Resto y aplicaciones a RSA. Algoritmos de Factorización de enteros.
4. ElGamal y el problema del logaritmo discreto. Algoritmos para resolver el problema del logaritmo discreto.
5. Funciones de Hash y aplicaciones. Familia SHA de funciones de Hash.
6. Firmas Digitales. Algoritmos de firmas digitales.
7. Criterios de seguridad basados en complejidad. Seguridad computacional de firmas digitales y encriptado.
8. Números pseudoaleatorios
9. Manejo de claves e infraestructura de clave pública (PKI).
10. Aplicaciones.

6. BIBLIOGRAFÍA

Tema	Básica	Complementaria
Introducción	(1)	(2,3)
Criptosistemas básicos de clave privada. AES.	(1)	(2)
RSA y el problema de factorización.	(1)	(2)
ElGamal y el problema del logaritmo discreto.	(1)	(2)
Funciones de Hash y aplicaciones.	(1)	(2)
Firmas Digitales.	(1)	(2)
Criterios de seguridad basados en complejidad.	(1)	(2)
Números pseudoaleatorios	(1)	(2)

Manejo de claves e infraestructura de clave pública (PKI).	(1)	(2)
Aplicaciones	(1)	(3)

6.1 Básica

1. Joachim von zur Gathen (2015). CryptoSchool. Springer. ISBN-13: 978-3662484234.

   El libro es accesible por el portal Timbó.

6.2 Complementaria

2. Alfred J. Menezes, Paul C. van Oorschot y Scott A. Vanstone (2001). Handbook of Applied Cryptography, Fifth Edition. CRC Press ISBN: 0-8493-8523-7 (2001).

   En línea en http://cacr.uwaterloo.ca/hac/

7. CONOCIMIENTOS PREVIOS EXIGIDOS Y RECOMENDADOS

7.1 Conocimientos Previos Exigidos:

Matemáticas Discretas

7.2 Conocimientos Previos Recomendados:

Probabilidad, Álgebra, Estructuras de Datos y Algoritmos.

ANEXO A

A1) INSTITUTO

Instituto de Computación.

A2) CRONOGRAMA TENTATIVO

Consiste en un cronograma de avance semanal con detalle de las horas de clase asignadas a cada tema.

Semana 1	Introducción y motivación histórica de la criptografía (4 hs.)
Semana 2	Criptosistemas básicos de clave simétrica (2 hs.) AES (2 hs.)
Semana 3	Práctico 1 y Obligatorio 1 (2 hs.) Diffie-Hellman y acuerdos de Claves (2 hs.)
Semana 4	Criptosistemas de clave pública y RSA (2 hs.) Análisis de seguridad de RSA (2 hs.)
Semana 5	Test de Primalidad y generación de números primos seguros (2 hs.) Teorema Chino del Resto y aplicaciones a RSA (2 hs.)
Semana 6	Algoritmos de Factorización de enteros (2 hs.) Práctico 2 (2 hs.)
Semana 7	Criptografía en grupos y el problema del logaritmo discreto (2 hs.) Criptosistema, ElGamal (2 hs.)
Semana 8	Algoritmos para resolver el problema del logaritmo discreto (4 hs.)
Semana 9	Práctico 3 (2 hs.) Funciones de Hash (2 hs.)
Semana 10	Familia SHA de funciones de Hash (2 hs.) Firmas digitales (2 hs.)
Semana 11	Algoritmos de firmas digitales y criterios de seguridad (2 hs.) Criterios de seguridad basados en complejidad (2 hs.)
Semana 12	Seguridad computacional de firmas digitales y encriptado (2 hs.) Práctico 4 y Obligatorio 2 (2 hs.)
Semana 13	Números Pseudoaleatorios (4 hs.)
Semana 14	PKI (4 hs.)
Semana 15	Aplicaciones(4 hs.)

A3) MODALIDAD DEL CURSO Y PROCEDIMIENTO DE EVALUACIÓN

Este es un curso exigente y con alta participación estudiantil en las clases. En general se va a mencionar en la clase anterior el material a leer, y en la clase siguiente se realizará una interacción con los estudiantes para responder dudas y relacionar los temas leídos con los ya vistos anteriormente (o incluso en otros cursos de la carrera). Al final se redondeará la clase resumiendo los conceptos más importantes.

En las clases donde discutimos ejercicios de los obligatorios se seguirá con la misma metodología. De ser necesario se fijará alguna clase extra especial de consultas de los ejercicios obligatorios.

La evaluación final se realizará mediante la resolución de ejercicios sacados del libro de texto consistiendo en 4 obligatorios (15 % cada uno), y 2 laboratorios con entrega de informe (20% cada uno).

Es importante aclarar que la participación en clase es obligatoria (con un 80% mínimo de asistencia), debido a que la metodología usada es fundamental para la comprensión de los temas dictados en el curso.

El curso se aprueba si se tiene el 60% o más de puntos y un 80% de asistencia a clase.

A4) CALIDAD DE LIBRE

Este curso no adhiere a resolución del consejo sobre condición de libre.

A5) CUPOS DE LA UNIDAD CURRICULAR

Este curso no tiene cupos.

ANEXO B para las carreras Ingeniería em Computación (plan 97) y Licenciatura en Computación

B1) ÁREA DE FORMACIÓN

Arquitectura, Sistemas Operativos y Redes.

B2) UNIDADES CURRICULARES PREVIAS

Para el Curso: exámenes aprobados de:
Matemática Discreta 1 y
Matemática Discreta 2 y
Programación 3.

Para el Examen: no aplica.