CARTA DESCRIPTIVA (FORMATO MODELO EDUCATIVO UACJ VISIÓN 2020)

I. Identificadores de la asignatura

Instituto: **INSTITUTO DE INGENIERÍA Y TECNOLOGÍA**

Modalidad: PRESENCIAL

Departamento: **FÍSICA Y MATEMÁTICAS**

Créditos: 8

Materia: **CRIPTOGRAFÍA**

Programa: **LIC EN MATEMATICAS**

Carácter: OPTATIVA

Clave:

Tipo: CURSO

Nivel: **AVANZADO**

Horas: **64 HRS** **Teoría:** 80% **Práctica:** 20%

II. Ubicación

Antecedentes: Clave

ALGEBRA MODERNA I

Consecuente:

NINGUNO

III. Antecedentes	
Conocimientos:	CONCEPTOS Y TEOREMAS BÁSICOS DE ALGEBRA ABSTRACTA.
Habilidades:	INVESTIGAR, ESTUDIO INDIVIDUAL, DISCUTIR Y TRABAJO EN EQUIPO.
Actitudes y valores:	Puntualidad, asistencia, responsabilidad, honestidad, superación y pensamiento crítico.

IV. Propósitos Generales
Los propósitos fundamentales del curso son:
PRESENTAR LOS CONCEPTOS, DEFINICIONES Y TEOREMAS BÁSICOS DE LA CRIPTOGRAFIA MATEMATICA.

V. Compromisos formativos

Intelectual: El estudiante comprenderá y sintetizará los conceptos primordiales acerca de la criptografía matemática. Conocerá las diferentes técnicas de cifrado y su fundamento matemático. Comprenderá los fundamentos del criptosistema RSA y el uso de curvas elípticas en los criptosistemas.

Humano: El estudiante reflexionará acerca de las implicaciones éticas de una formación científica y de una forma de razonamiento crítico fundamentados en la adquisición de conocimientos con significado (tanto abstractos como específicos).

Social: El estudiante reflexionará acerca de las implicaciones de una formación científica y de una forma de razonamiento crítico fundamentados en la adquisición de conocimientos con significado (tanto abstractos como específicos) en la sociedad mexicana.

Profesional:

El estudiante incorporará a su formación profesional los elementos fundamentales de la Criptografía de tal manera que sea capaz de aplicarlos en otras áreas del conocimiento científico.

VI. Condiciones de operación

Espacio: AULA TRADICIONAL

Laboratorio: CÓMPUTO

Población: 3-20

Mobiliario:

A) Mesabanco
B) Sillas

Material de uso frecuente:

A) Laptop
B) Cañon Proyector
c) Marcadores para Pizarron Blanco.

Condiciones especiales: No Aplica

VII. Contenidos y tiempos estimados		
Temas	Contenidos	Actividades
UNIDAD I CONCEPTOS BÁSICOS (16 hrs) (4 sem)	1.1 Historia de la Criptografía. 1.2 Cifrado por Sustitución Simple. 1.3 Divisibilidad y Máximo Común Divisor. 1.4 Aritmética Modular. 1.5 Números Primos, Factorización Única y Campos Finitos. 1.6 Potencias y Raíces Primitivas en Campos Finitos.	Presentación del curso. Exposición de las definiciones, teoremas y demostraciones así como de ejemplos relevantes a la temática de esta unidad. Retroalimentación al final de la unidad.
UNIDAD II CRIPTOGRAFÍA DE CLAVE PÚBLICA (16 hrs) (4 sem)	2.1 Ideas Básicas de la Criptografía de Clave Pública. 2.2 El Problema del Logaritmo Discreto (PLD). 2.3 Intercambio de Claves Diffie-Hellman. 2.4 El Criptosistema de Clave Pública ElGamal. 2.5 Repaso de Teoría de Grupos, y Teoría de Anillos. 2.6 Intentando Resolver el PLD: Fuerza Bruta, Algoritmo de Colisión y Pohlig-Hellman.	Exposición de las definiciones, teoremas y demostraciones así como de ejemplos relevantes a la temática de esta unidad. Retroalimentación al final de la unidad.
UNIDAD III EL CRIPTOSISTEMA RSA (16 hrs) (4 sem)	3.1 La Fórmula de Euler y Raíces módulo pq. 3.2 El Criptosistema de Clave Pública RSA. 3.3 Algunos Test de Primalidad. 3.4 Algoritmo de Pollard. 3.5 Factorización por Diferencial de Cuadrados.	Exposición de las definiciones, teoremas y demostraciones así como de ejemplos relevantes a la temática de esta unidad. Retroalimentación al final de la unidad.

UNIDAD IV CURVAS ELÍPTICAS Y CRIPTOGRAFÍA (16 hrs) (4 sem)	4.1 Curvas Elípticas. 4.2 Curvas Elipticas sobre Campos Finitos. 4.3 El PLD en Curvas Elípticas 4.4 Criptografía en Curvas Elípticas. 4.5 El Algoritmo de Factorización de Lenstra.	Exposición de las definiciones, teoremas y demostraciones así como de ejemplos relevantes a la temática de esta unidad. Retroalimentación al final de la unidad.

VIII. Metodología y estrategias didácticas

Metodología Institucional:

a) Elaboración de ensayos, monografías e investigaciones (según el nivel) consultando fuentes bibliográficas, hemerográficas y en Internet.
b) Elaboración de reportes de lectura de artículos en lengua inglesa, actuales y relevantes.

Estrategias del Modelo UACJ Visión 2020 recomendadas para el curso:

a) Búsqueda, Organización y Recuperación de Información.
b) Comunicación Horizontal.
c) Descubrimiento.
d) Ejecución-Ejercitación
e) Elección, Decisión.
f) Evaluación.
g) Extrapolación y Transferencia.
h) Internalización
i) Investigación.
j) Trabajo Colaborativo
k) Proceso de Pensamiento Lógico y Crítico.
l) Significado, Generalización.
m) Análisis y Síntesis.
n) Aprendizaje Significativo.

IX. Criterios de evaluación y acreditación

a) Institucionales de acreditación:

Acreditación mínima de 80% de clases programadas

Entrega oportuna de trabajos

Calificación ordinaria mínima de 7.0

Permite examen único: no ☐ si ☑

b) Evaluación del curso

Acreditación de los temas mediante los siguientes porcentajes:

Unidad I	10%
Unidad II	10%
Unidad III	10%
Unidad IV	10%
Participación	10%
Tareas	20%
Examen Final	30%
TOTAL	100%

X. Bibliografía

Nota: Revisar la bibliografía obligatoria y complementaria, así como citar adecuadamente según sea el caso de libros, revistas, páginas electrónicas, compilaciones, libros electrónicos, etc.

BIBLIOGTRAFIA OBLIGATORIA.
J. Hoffstein, J. Pipher, J. Silverman, "An Introduction to Mathematical Cryptography". 2nd Ed, Springer 2014.

BIBLIOGRAFIA EN LENGUA INGLESA.
G. Baumslag, B. Fine m. Kreuzer, "A Course in Mathematical Cryptography". Walter de Gruyter GmbH 2015.

BIBLIOGRAFIA COMPLEMENTARIA Y DE APOYO.
L C. Washington, "Elliptic Curves, Number Theory and Cryptography", 2nd Ed. Chapman & Halla/CRC.

XI. Perfil deseable del docente

Conocimiento en la materia, experiencia docente y estudios de posgrado, preferentemente en el área de matemática pura.

XII.Institucionalización

Responsable del Departamento: M. en C. Natividad Nieto

Coordinador/a del Programa: M. en C. Pedro López Hernández

Fecha de elaboración: Mayo 2016

Elaboró: Dr. Oscar H. Estrada Estrada

Fecha de rediseño: Febrero 2016

Rediseñó: Dr. Oscar H. Estrada Estrada