# PROGRAMA ANALÍTICO DE ASIGNATURA

## 1. IDENTIFICACION DE LA MATERIA

**NOMBRE DE LA ASIGNATURA**: Criptografía y Seguridad
**PRE-REQUISITOS** : Electiva
**SIGLA Y CODIGO** : ELC107
**NIVEL** : Octavo Semestre
**HORAS** : 4 (3HT - 1HP)
**CREDITOS** : 5
**REVISADO EN** : Agosto 2011

## 2. JUSTIFICACIÓN

**"**Cada vez utilizamos más los sistemas de transacción o intercambios de información a distancia porque nos facilitan mucho la vida y nos dan un alcance que antes no teníamos, pero si esto nos va a provocar problemas como que otras personas utilicen nuestras cuentas bancarias, esta herramienta se va a poder". Como podemos observar en la cita anterior, muchas personas temen utilizar los servicios "en línea" que muchas empresas ofrecen para poder realizar sus pagos, hacer transacciones o algún tipo de servicio que se relacione con en manejo de dinero, ya que lo consideran inseguro. Es aquí donde la criptografía entra en juego para cambiar este pensamiento, que no es en su totalidad incorrecto. Si se utilizan las herramientas que nos brindan la criptografía se podría considerar realizar transacciones "en línea" como una forma tan segura como ir en persona al banco. La única barrera que existe hoy en día, es que las personas se den cuenta de la dificultad que es obtener información que se encuentra encriptada correctamente.

Aunque es poco probable que un profesional de las Ciencias de la Computación, desarrolle un nuevo criptosistema, él debería ser capaz de entender los algoritmos

utilizados en su ámbito profesional y poder evaluar las fortalezas y debilidades de los mismos.

Por tanto Obtendrá la capacidad de abstracción para explicar en forma procedimental, un método de encriptación, Desarrollara la capacidad de aplicar de control de seguridad en sistemas informáticos de acuerdo a las necesidades; Implementara y analizara Herramientas de apoyo en proceso de protección de la información.

## 3. OBJETIVOS DE LA ASIGNATURA

### 3.1. OBJETIVOS GENERAL

Comprender y Desarrollar Técnicas para resguardar los sistemas informáticos, aplicando los conceptos teóricos de los algoritmos mas conocidos de criptografía, el curso, el alumno será capaz de comprender y/o utilizar los algoritmos más conocidos de la Criptografía.

### 3.2. OBJETIVOS ESPECIFICOS

- Comprender la aritmética modular, resaltando su importancia en el ámbito de la programación.
- Analizar los distintos criptosistemas de cifra simétrica y asimétrica, observando el uso de las mismas en transacciones seguras.
- Describir e interpretar los conceptos de Amenazas, vulnerabilidad y riesgos en forma oral y escrita.
- Describir e interpretar los mecanismos para seguridad lógica de la información.

- Describir e interpretar el funcionamiento de las principales técnicas para garantizar la confidencialidad, integridad, y disponibilidad de la información.

## 4. CONTENIDO MINIMO

Conceptos Básicos de la Seguridad Informática, Principios de la Criptografía, Criptología, Criptoanalisis, Teoría Matemática aplicada a la Criptografía, Criptografía Clásica, Cifradores en Flujo, Cifradores en Bloque, Funciones Hash y Firma Digital.

## 5. UNIDADES DEL PROGRAMA ANALITICO

**UNIDAD I : CONCEPTOS TEORICOS**

**TIEMPO : 24 HORAS**

**OBJETIVOS:**

El estudiante tendra la capacidad de explicar de forma clara el funcionamiento de los diferentes algoritmos matemáticos.

**2 Conceptos Básicos.**

Criptografía.
Confidencialidad e Integridad
Criptosistemas Simétricos
Criptosistemas Asimétricos
Seguridad Informática
Amenazas
Vulnerabilidad
Elementos de Seguridad de la Información

**3 Teoría de los números.**

Teoría de la información.

Aritmética Modular.

Divisibilidad de los números.

Inversos de un Cuerpo.

Función de Euler

Teorema del Resto chino.

Algoritmo de exponenciación rápida.

**UNIDAD II : CRIPTOGRAFIA CLASICA**

**TIEMPO : 16 HORAS**

**OBJETIVOS:**

El estudiante describirá los eventos transcendentales en la evolución de la criptografía hasta antes de la aparición de las computadoras.

**2 <u>Historia.</u>**

Eventos Históricos

Clasificación de los sistemas de cifra clásica.

Cifrador Excítala.

Cifrador de Polybios.

Cifrador por Transposición.

Cifrador por Sustitución (Mono alfabéticos y Poli alfabéticos)

**UNIDAD III : CRIPTOGRAFIA MODERNA**

**TIEMPO : 24 HORAS**

**OBJETIVOS:**

El estudiante comprenderá la forma de cifrados en flujo y los generadores Pseudoaleatorios, Cifradores en bloque y sus modos y los tipos de funciones Hash y su evolución hasta el uso de la firma digital.

**2 Cifrado en Flujo.**

Cifrador de Flujo Básico.

Rachas de Dígitos.

Generador de Congruencia lineal.

Registro de Desplazamientos.

Generadores Lineales – LFSR.

Algoritmos – A5/1 , A5/2

**3 Cifrado en Bloque.**

Cifrador Tipo Feistel.

Data Encription Standard.

Cajas S en DES.

Modos de Cifra ECB, CBC, CFP.

AES, Algoritmos Rijndael.

Esquema general de AES y sus Funciones

**4 Funciones Hash.**

Propiedades de la Funciones Hash

Funciones MAC (MD5, SHA1, SHA2).

Funciones MDC.

**5 Autenticación y Firma Digital.**

Problemas de Integridad

Autenticación con sistemas simétricos

Autenticación con sistemas Asimétricos

## 6. METODOLOGIA

**Medios de Enseñanza:**

Libros, Computador (Lenguajes de Programación, Sitios Web en Internet),, Reproductor Multimedia y Pizarra (Acrílica) Marcadores de agua, Herramientas de Software y Simulación .

**Estrategias de Enseñanza y de Aprendizaje:**

Métodos Expositivo, Demostrativo

Métodos Asociativo

Búsqueda y Elaboración de Significados de Conceptos

Trabajos en Grupos, y Organización de la Información.

Imitación de Modelos.

Caso de Estudios de Ejemplos de la vida real.

## 7. CRONOGRAMA

| SEMANA / ACTIVIDADES | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Presentación | | | | | | | | | | | | | | | | | | |
| Unidad I | | | | | | | | | | | | | | | | | | |
| 1er Parcial | | | | | | | | | | | | | | | | | | |
| Unidad II | | | | | | | | | | | | | | | | | | |
| 1er Proyecto | | | | | | | | | | | | | | | | | | |
| Unidad III | | | | | | | | | | | | | | | | | | |
| 2do Parcial | | | | | | | | | | | | | | | | | | |
| 2do Proyecto | | | | | | | | | | | | | | | | | | |

## 8. EVALUACION

**1 Tipos y Momentos.**

- Antes de la Enseñanza: Diagnósticos del estado de los conocimientos adquiridos con anterioridad
- Durante la Enseñanza: Interactiva ejercicios de conocimiento general en el punto de análisis del problema, Retroactiva ejercicios que sirve como base para la solución de otros problemas(generalización)
- Después de la Enseñanza: Balance de los resultados Obtenidos, mediante métodos acumulativos.

**2 Componentes de la Evaluación**

- Pruebas de respuestas breves, respuesta guiada, elección múltiple.
- Pruebas de Resolución de Problemas.
- Pruebas de habilidad Practica, Observación.

**3 Calificación**

Asignación de un valor "Cuantitativo-Cualitativo" a los resultados de la evaluación.

**a) Ponderación Parciales (50%)**

b) **Primera Evaluación** **(25%)** (Unidad I)

- Participación Oral 02 %
- Participación Practica 03 %
- Evaluación 20 %

c) **Segunda Evaluación** **(25%)** (Unidad II, III)

- Participación Oral 02 %
- Participación Practica 03 %
- Evaluación 20 %

d) **Ponderación Proyectos** **(50%)**

(Unidad I, III)

- Presentación Documentación 10 %
- Defensa del proyecto 15 %
- Aspectos Técnicos 25 %

## 9. BIBLIOGRAFÍA

- Schneier, Bruce. APPLIED CRYPTOGRAPHY: PROTOCOLS; ALGORITMS AND SOURCE CODE IN C, Second Edition, Jhon Wiley, 1996

- Group-based Cryptography (Advanced Courses in Mathematics - CRM Barcelona) ,183 Paginas,Birkhäuser Basel; 1 edition (August 27, 2008)

- La Criptografía como elemento de la seguridad informática. (Spanish). *ACIMED* [serial online]. November 2003;11(6):90-97. Available from: Fuente Académica, Ipswich, MA. Accessed February 25, 2010. http://search.ebscohost.com/login.aspx?direct=true&db=zbh&AN=26302695&lang=es&site=ehost-live

- Molina Mateos, José María. Seguridad de la información. Criptología. , , Argentina: El Cid Editor, 2000. p 8. http://site.ebrary.com/lib/uagrmsp/Doc?id=10018530&ppg=8 Copyright © 2000. El Cid Editor. All rights reserved.

- Morant Ramón, J.L.; Ribagorda Garnacho, A; Sancho Rodríguez J. SEGURIDAD Y PROTECCION DE LA INFORMACION Colección de Informática, Editorial Centro de Estudios Ramón Areces, S.A., Madrid 1994
- Menezes, Alfred; Oorsschof, Paul; Vanstone, Scott. HANDBOOK OF APPLIED CRYPTOGRAPHY. CRC Press Inc 1997
- Scrneier, Bruce. APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C. Second edition, Jhon Wiley & sons, Inc., New York, 1996
- Douglas R. stinson. CRYPTOGRAPHY. THEORY AND PRACTICE. Third edition, Champan & Hall/ CRC,2006