Universidad de Guadalajara
Centro Universitario de los Lagos

PROGRAMA DE ESTUDIO
FORMATO BASE

1. IDENTIFICACIÓN DEL CURSO

Nombre de la materia

Criptografía

Clave de la materia:	Horas de teoría:	Horas de práctica:	Total de Horas:	Valor en créditos:
I0222	**48**	**16**	**64**	**7**

Tipo de curso: (Marque con una X)											
C= curso	**X**	P= practica		CT = curso–taller		M= módulo		C= clínica		S= seminario	

Nivel en que se ubica: (Marque con una X)			
L=Licenciatura	**X**	P=Posgrado	

Prerrequisitos formales (Materias previas establecidas en el Plan de Estudios)	Prerrequisitos recomendados (Materias sugeridas en la ruta académica aprobada)

Departamento:

Ciencias Exactas y Tecnología

Carrera:

LIEC

Área de formación:

Área de formación básica común obligatoria.		Área de formación básica particular obligatoria.		Área de formación básica particular selectiva.		Área de formación especializante selectiva.	**X**	Área de formación optativa abierta.	

Historial de revisiones:

Acción: Revisión, Elaboración	Fecha:	Responsable
Elaboración	**Enero de 2012**	**Dr. Héctor Alfonso Juárez López**

Academia:

Cómputo

Aval de la Academia:

Enero de 2012		
Nombre	**Cargo**	**Firma**
Lic. Auria Lucía Jiménez Gutiérrez	**Presidente**	

2. PRESENTACIÓN

El presente curso presenta al alumno las técnicas y principios más comunes de la criptografía. Se revisan los elementos básicos de los sistemas criptográficos y de la seguridad en redes de computadoras.

3. OBJETIVO GENERAL

El alumno conocerá los elementos básicos de un sistema criptográfico, será capaz de analizar e implementar sistemas criptográficos tanto de clave simétrica como de clave abierta y describirá los principales elementos en un sistema de seguridad para redes de computadoras.

4. OBJETIVOS ESPECÍFICOS

Que el alumno conozca los elementos básicos de un sistema criptográfico
Que el alumno conozca e implemente técnicas de cifrado de clave simétrica
Que el alumno conozca e implemente técnicas de cifrado de clave abierta
Que el alumno conozca técnicas estándar de codificación, como DES, AES, RSA, PGP, etc.

5. CONTENIDO

Temas y Subtemas

1. **Presentación del Curso**
   a) Tendencias en la seguridad
   b) La arquitectura de seguridad OSI
   c) Ataques, servicios y mecanismos de seguridad
2. **Técnicas clásicas de cifrado**
   a) Cifrado simétrico
   b) Substitución
   c) Transposición
   d) Máquinas de cifrado
3. **DES y AES**
   a) Cifrado en bloques
   b) DES
   c) Análisis de DES
   d) Elementos básicos de Teoría de números
   e) AES
   f) Análisis de AES
4. **Aspectos de cifrado simétrico**
   a) Cifrado múltiple y triple DES
   b) Cifrado de flujo
   c) Seguridad de los canales de comunicación
   d) Distribución de llaves

e) Generación de números aleatorios

5. Cifrado de clave abierta

a) Algoritmos de teoría de números
b) Principios de un sistema de clave abierta
c) RSA
d) Cifrado con curvas elípticas

6. Autentificación

a) Funciones de autentificación
b) Códigos de autentificación
c) Funciones Resumen
d) Algoritmos HASH y MAC
e) Firmas digitales
f) Protocolos de autentificación

7. Aplicaciones

a) Kerberos
b) PGP
c) S/MIME
d) Seguridad en IP
e) Aspectos generales de seguridad en WEB

7. TAREAS, ACCIONES Y/O PRÁCTICAS DE LABORATORIO

a) Aprendizaje individual, grupal y autogestivo.
b) Integración individual de productos de aprendizaje (reportes de lectura, proyectos de programación, ensayos, formatos de intervención, trabajos de investigación, presentaciones, entre otros).

8. BIBLIOGRAFÍA BÁSICA (Preferentemente ediciones recientes, 5 años)

1	William Stallings, *Cryptography and Network Security: Principles and Practice*, 5ª ed, Prentice Hall, 2011
2	David Hook, *Beginning Cryptography with Java*, Wrox Press, 2005
3	Nichols, Randall K. *Seguridad para comunicaciones inalámbricas : redes, protocolos, criptografía y soluciones*, McGraw-Hill, 2003
4	Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone, *Handbook of applied cryptography*, 5th ed, CRC Press, 2001
5	

9. BIBLIOGRAFÍA COMPLEMENTARIA (Preferentemente ediciones recientes, 5 años)

1	Levy, Steven, *Cripto : cómo los informáticos libertarios vencieron al gobierno y salvaguardaron la intimidad*, Alianza editorial, 2002
2	Fúster Sabater, Luis,*Técnicas criptográficas de protección de datos*, Alfaomega, 2001
3	Cobb, Chey, *Cryptography for dummies*, For Dummies, 2004
4	
5	

10. CRITERIOS Y MECANISMOS PARA LA ACREDITACION

Acreditación: Para tener derecho a examen ordinario el alumno deberá cumplir con un 80% de las asistencias y para tener derecho a examen extraordinario el alumno deberá cumplir con el 60% de las asistencias.

11. EVALUACIÓN Y CALIFICACIÓN

Unidad de Competencia:	Porcentaje:
Examen Departamental	35.00%
Exámenes Ordinarios	35.00%
Productos de Práctica	30.00%