INSTITUTO POLITÉCNICO NACIONAL

SECRETARIA DE INVESTIGACIÓN Y POSGRADO

DIRECCIÓN DE POSGRADO

FORMATO GUÍA PARA REGISTRO DE ASIGNATURAS

I. DATOS DEL PROGRAMA Y LA ASIGNATURA

1.1 NOMBRE DEL PROGRAMA: **MAESTRÍA EN TECNOLOGÍA DE CÓMPUTO**

1.2 COORDINADOR DEL PROGRAMA: **DR. JUAN CARLOS HERRERA LOZADA**

1.3 NOMBRE DE LA ASIGNATURA: **SISTEMAS CRIPTOGRÁFICOS**

1.4 CLAVE: 08A5377 (Para ser llenado por la SIP)

1.5 TIPO DE ASIGNATURA:

OBLIGATORIA		OPTATIVA	X
SEMINARIO		ESTANCIA	

1.6 NÚMERO DE HORAS: **72**

TEORÍA	PRACTICA	T-P
4		

1.7 UNIDADES DE CRÉDITO: **8**

1.8 FECHA DE LA ELABORACIÓN DEL PROGRAMA DE LA ASIGNATURA:

13	05	2013
d	m	A

1.9 SESIÓN DEL COLEGIO DE PROFESORES EN QUE SE ACORDÓ LA IMPLANTACIÓN DE LA ASIGNATURA:

SESIÓN No.	7a. Ext.	FECHA:	12	06	2013
			d	m	a

1.10 FECHA DE REGISTRO EN SIP:

d	M	a

(Para ser llenado por la SIP)

II. DATOS DEL PERSONAL ACADÉMICO

2.1	COORD. ASIGNATURA:	DR. VÍCTOR MANUEL SILVA GARCÍA	CLAVE: 8813-ED-12
2.2	PROFR. PARTICIPANTE:	DR. ROLANDO FLORES CARAPIA	CLAVE: 7953-EC-11
		M. EN C. EDUARDO RODRÍGUEZ ESCOBAR	CLAVE: 8595-ED-12

III. DESCRIPCIÓN DEL CONTENIDO DEL PROGRAMA DE LA ASIGNATURA

III.1 OBJETIVO GENERAL:

Proporcionar a los alumnos las bases teóricas de los métodos criptográficos empleados desde la antigüedad hasta la aparición de las Teoría de la Información, con la finalidad de que el estudiante aprenda la terminología y metodología de esta ciencia para el aseguramiento de la información cuando ésta se transmite por medios inseguros o se almacena en dispositivos.

III.2 DESCRIPCIÓN DEL CONTENIDO

TEMAS Y SUBTEMAS	TIEMPO
1. Panorama histórico de la criptografía.	**6 Horas**
1.1 Primeros métodos criptográficos.	
1.2 Métodos criptográficos durante la edad media y el renacimiento.	
1.3 Métodos criptográficos en la época moderna.	
2. Criptosistemas	**18 Horas**
2.1 Objetivos de la criptografía	
2.2 Elementos que componen un criptosistema	
2.3 Tipos de criptosistemas	
2.4 Criptosistemas de clave secreta	
2.5 Criptosistemas de clave pública	
3. Funciones matemáticas de cifrado	**24 Horas**
3.1 Métodos de sustitución	
3.2 Métodos de permutación	
3.4 Métodos para la generación de claves secretas	
3.5 Métodos para la generación de claves públicas	
4. Tipos de cifrado	**24 Horas**
4.1 Cifrado en Flujo	
4.2 Cifrado de bloques	
4.3 Nuevos métodos de cifrado	

III.3 BIBLIOGRAFIA UTILIZADA EN LA ASIGNATURA

1.- Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley;

2nd edition, ISBN-10: 0471117099, USA 1996.

2.- Niels Ferguson, Bruce Schneier , Cryptography Engineering: Design Principles and Practical Applications, Wiley; 1 edition, ISBN-10: 0470474246, USA 2010

3.- Stinson Douglas R, Cryptography Theory and Practice, Chapman & Hall/CRG; Third edition, BN-10: 1584885084, USA 2005.

4.- Stallings William, Cryptography and Network Security: Principles and Practice, Prentice Hall,

5 edition, ISBN-10: 0136097049, 2010.

5.- Menezes Alfred, Van Oorschot Paul C, A. Vanstone Scout, Handbook of Appled Criptografhy, CRC Press; 1 edition, ISBN-10: 0849385237, 1996.

III.4 PROCEDIMIENTOS O INSTRUMENTOS DE EVALUACIÓN A UTILIZAR

Examen 50%

Tareas 10%

Participación en clase 10%

Proyecto 30%