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: **CRIPTOGRAFÍA APLICADA**

1.4 CLAVE: 08A5376 (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:

15	04	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. ROLANDO FLORES CARAPIA	CLAVE:	7953-EC-11
2.2	PROFR. PARTICIPANTE:	DR. VÍCTOR MANUEL SILVA GARCÍA	CLAVE:	8813-ED-12
		M. EN C. EDUARDO RODRÍGUEZ ESCOBAR	CLAVE:	8595-ED-12

III. DESCRIPCIÓN DEL CONTENIDO DEL PROGRAMA DE LA ASIGNATURA

III.1 OBJETIVO GENERAL:

Proporcionar al alumno los conocimientos teóricos para la implementación de protocolos criptográficos Basados en sistemas simétricos y asimétricos así como sus aplicaciones.

III.2 DESCRIPCIÓN DEL CONTENIDO

TEMAS Y SUBTEMAS	TIEMPO
1.- Algoritmos criptográficos	**16 Horas**
1.1 Algoritmos de llave pública	
1.2 Data Encryption Standard (DES)	
1.3 Advanced Encryption Standard (AES)	
2.- Algoritmos de llave pública para firma digital	**16 Horas**
2.1 Esquemas de identificación	
2.2 Algoritmos de cambio de llave	
2.3 Algoritmos especiales para protocolos	
2.4 Funciones Hash	
3 Protocolos Criptográficos	**16 Horas**
3.1 Protocolos básicos	
3.2 Protocolos intermedios	
3.3 Protocolos avanzados	
4.- Casos prácticos	**24 Horas**
4.1 Ejemplos e Implementación	
4.2 Políticas	

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.- Christof Paar, Jan Pelzl, Bart Preneel, Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 1st edition, ISBN-10: 3642041000, 2010.

III.4 PROCEDIMIENTOS O INSTRUMENTOS DE EVALUACIÓN A UTILIZAR

Examen 50%

Tareas 10%

Participación en clase 10%

Proyecto 30%