INSTITUTO POLITÉCNICO NACIONAL
SECRETARÍA ACADÉMICA
DIRECCIÓN DE ESTUDIOS PROFESIONALES

ESCUELA: UNIDAD PROFESIONAL INTERDISCIPLINARIA EN INGENIERÍA Y TECNOLOGÍAS AVANZADAS **CARRERA: INGENIERÍA TELEMÁTICA** **ESPECIALIDAD:** **COORDINACIÓN: ACADEMIA DE TELEMÁTICA** **DEPARTAMENTO:**	**ASIGNATURA: SEGURIDAD DE DATOS** **CLAVE: ITSEGD1084 SEMESTRE: DÉCIMO** **CREDITOS: 6 VIGENTE: ENERO 2001** **TIPO DE ASIGNATURA: TEORICO/PRÁCTICA** **MODALIDAD: ESCOLARIZADA**

FUNDAMENTACIÓN DE LA ASIGNATURA

En la actualidad el manejo de grandes cantidades de información, procesamiento y su transferencia de un punto a otro se ha vuelto una necesidad para las grandes compañías, el medio utilizando para estos fines es una Red de Telecomunicaciones (sea pública o privada) de amplia cobertura y requieren de sistemas para garantizar la confidencialidad de la comunicación y la autenticidad de la información recibida en el destino. La materia de Seguridad de Datos le proporciona al Ingeniero en Telemática las herramientas necesarias para el entendimiento, desarrollo, implementación y manejo de las técnicas y algoritmos utilizados para lograr una comunicación de datos segura. Para lograr lo anterior el profesor expondrá de manera detallada las herramientas necesarias al alumno y recurrirá intensivamente a las tareas para que el alumno desarrolle e implemente los algoritmos en la computadora. Por lo anterior es necesario que el alumno poséa previamente algunas herramientas que le serán útiles y que se le han proporcionado en cursos anteriores como lo son Programación en Lenguaje C, Análisis y Diseño de Algoritmos, Redes de Computadoras y Arquitectura de Computadoras, así como algunos conceptos introductorios de campos y su álgebra asociada como soporte matemático para algunos de los algoritmos de criptografía. Esta asignatura está diseñada como parte final de la formación del Ingeniero en Telemática dentro de la U. P. I. I. T. A., y en algunos casos le será de gran utilidad en el desarrollo de su Trabajo Terminal y en su ejercicio profesional.

OBJETIVO DE LA ASIGNATURA

- El alumno identificará, analizará y evaluará las principales técnicas y algoritmos de encriptamiento, y las aplicará en sistemas de transferencia de información en un medio público como una red de cobertura amplia, con el fin de proporcionar confidencialidad y autenticidad a la comunicación.

TIEMPOS TOTALES ASIGNADOS: **HRS/SEMESTRE: 60 HRS/SEMANA: 4** **HRS/TEORÍA/SEMESTRE: 30** **HRS/PRÁCTICA/SEMESTRE: 30**	**PROGRAMA ELABORADO O ACTUALIZADO POR:** **ACADEMIA DE TELEMÁTICA** **REVISADO POR: SUBDIRECCIÓN ACADÉMICA** **APROBADO POR: C.T.C.E./12 DE MARZO/99**	**AUTORIZADO POR: LA COMISIÓN DE PLANES Y PROGRAMAS DE ESTUDIO DEL C. G. C. / 24 DE MAYO DE 1999**

No. UNIDAD: I **NOMBRE: INTRODUCCIÓN A LA SEGURIDAD Y A LA CRIPTOGRAFÍA**

OBJETIVOS PARTICULARES DE LA UNIDAD

- El alumno analizará el problema que se presenta al establecer medidas de seguridad en los sistemas de transmisión de datos; identificará algunos casos típicos reales en donde resulta imprescindible un sistema de seguridad (instituciones financieras, empresas, bancos, etc.).
- El alumno identificará los principales conceptos y definiciones que se manejan en el ramo.

# DE TEMA	TEMAS	INSTRUMENTACIÓN DIDÁCTICA	H/T	H/P	E.C.	CLAVE
1.1	**Introducción.** 1.1.1 Planteamiento del problema. 1.1.2 Ataques a la seguridad de un sistema o una red. 1.1.3 Servicios de seguridad.	Exposición frente a grupo utilizando el pizarrón y acetatos. Realización de tareas por parte de los alumnos.	1	0	1	1B, 2B, 4C, 6C, 7C
1.2	**Conceptos.** 1.2.1 Criptoanálisis. 1.2.2 Criptografía. 1.2.3 Secrecía. 1.2.4 Sistema con secrecía perfecta.		1		1	
		SUBTOTAL	2	0	2	

No. UNIDAD: II **NOMBRE: CRIPTOGRAFÍA CONVENCIONAL**

OBJETIVOS PARTICULARES DE LA UNIDAD

- El alumno analizará los algoritmos para realizar criptografía convencional de datos, comparará las ventajas y desventajas de cada uno de ellos y en que sistemas de procesamiento y/o transmisión de información se utilizan por sus características.
- El alumno analizará con detalle el algoritmo estándar de encriptamiento de datos y las características que lo hacen apropiado para una gran variedad de aplicaciones de procesamiento y/o transferencia de información.

# DE TEMA	TEMAS	INSTRUMENTACIÓN DIDÁCTICA	H/T	H/P	E.C.	CLAVE
2.1	**Modelo de criptografía convencional: sistemas con una llave.**	Exposición frente a grupo utilizando el pizarrón y acetatos.	1	0	1	1B, 3B, 4C, 7C
2.2	**Técnicas de encriptamiento clásico.** 2.2.1 Encriptamiento por substitución. 2.2.2 Encriptamiento por transposición. 2.2.3 Encriptamiento por flujo. 2.2.4 Encriptamiento por bloque.	Realización de tareas y programas de computadora implementando algunos de los algoritmos de encriptamiento visto en clase. Realización de prácticas de laboratorio.	2	4	2	
2.3	**Estándar de encriptado de datos (DES).** 2.3.1 Sensibilidad a errores. 2.3.2 Modos de operación.		2	5	2	
		SUBTOTAL	5	9	8	

No. UNIDAD: III **NOMBRE: CONFIDENCIALIDAD USANDO CRIPTOGRAFÍA CONVENCIONAL**

OBJETIVOS PARTICULARES DE LA UNIDAD

- El alumno analizará el grado de confidencialidad que se puede obtener con los algoritmos de encriptamiento convencional y la manera de administrar las llaves dentro de una red de comunicaciones para los algoritmos de llave privada como lo es DES.
- El alumno analizará y aplicará el procedimiento de asignación de llave para una sesión y su renovación.

# DE TEMA	TEMAS	INSTRUMENTACIÓN DIDÁCTICA	H/T	H/P	E.C.	CLAVE
3.1	**Localización de la función de encriptado.**	Exposición frente a grupo utilizando el pizarrón y acetatos.	1	0	1	3B, 4C, 7C
3.2	**Distribución de las llaves.**		1		1	
	3.2.1 El KDC.	Realización de tareas y programas de computadora implementando algunos de los algoritmos de distribución de llaves.				
	3.2.2 Procedimiento de asignación y cambio de llaves.					
		SUBTOTAL	2	0	2	

No. UNIDAD: IV **NOMBRE: SISTEMAS CRIPTOGRÁFICOS BASADOS EN LLAVES PÚBLICAS**

OBJETIVOS PARTICULARES DE LA UNIDAD

- El alumno identificará y analizará los algoritmos de encriptamiento basados en llave pública, y de entre ellos cubrirá a profundidad el algoritmo RSA, utilizando los conceptos básicos de la teoría de números y su uso en el algoritmo RSA.
- El alumno aplicará las diversas formas en que se administran las llaves de encriptamiento/decriptamiento del algoritmo RSA.

# DE TEMA	TEMAS	INSTRUMENTACIÓN DIDÁCTICA	H/T	H/P	E.C.	CLAVE
4.1	**Introducción a los sistemas criptográficos basados en llaves públicas.**	Exposición frente a grupo utilizando el pizarrón y acetatos.	1	1	1	1B, 2B, 3B, 4C, 7C
4.2	**El algoritmo RSA.** 4.2.1 Uso de RSA para llaves de DES. 4.2.2 Teoría de números.	Realización de tareas y programas de computadora implementando algunos de los algoritmos de encriptamiento visto en clase.	2	4	2	
4.3	**Administración de las llaves.**	Realización de prácticas de laboratorio.	1		1	
		SUBTOTAL	4	5	4	

No. UNIDAD: V **NOMBRE: AUTENTIFICACIÓN Y FIRMAS DIGITALES**

OBJETIVOS PARTICULARES DE LA UNIDAD

- El alumno evaluará la necesidad de autentificación en un sistema de transferencia y/o acceso a información.
- El alumno identificará las principales formas de implementar funciones de autentificación implementadas en sistemas de información actuales (como las firmas digitales y el PIN):

# DE TEMA	TEMAS	INSTRUMENTACIÓN DIDÁCTICA	H/T	H/P	E.C.	CLAVE
5.1	**Requerimientos de autentificación.**	Exposición frente a grupo utilizando el pizarrón y acetatos.	1	1	1	1B, 3B, 4C
5.2	**Técnicas de autentificación.**		1	2	1	
	5.2.1 Firmas digitales.	Realización de tareas y programas de computadora implementado algunos de los algoritmos de autentificación.				
	5.2.2 Sistemas de transferencias de fondos y el PIN.					
		Realización de prácticas de laboratorio.				
		SUBTOTAL	2	3	1	

No. UNIDAD: VI **NOMBRE: INTRUSOS, VIRUS Y GUSANOS**

OBJETIVOS PARTICULARES DE LA UNIDAD

- El alumno identificará las principales formas de accesos no autorizados a la red de comunicación y a los sistemas de información, cómo detectarlos y algunas de las posibles acciones a tomar para evitarlos.
- El alumno analizará algunas de las principales características que hacen de una red y/o un sistema de información vulnerable a ataques externos a la red o al sistema.

# DE TEMA	TEMAS	INSTRUMENTACIÓN DIDÁCTICA	H/T	H/P	E.C.	CLAVE
6.1	**Intrusos y detección de intrusos.** 6.1.1 Passwords y su vulnerabilidad.	Exposición frente a grupo utilizando el pizarrón y acetatos.	1	0	1	1B, 2B
6.2	**Virus.**	Realización de tareas por parte de los alumnos.	1		1	
6.3	**Gusanos.**		1		1	
		SUBTOTAL	3	0	2	

No. UNIDAD: VII **NOMBRE: OTROS ALGORITMOS CRIPTOGRÁFICOS**

OBJETIVOS PARTICULARES DE LA UNIDAD

- El alumno analizará y evaluará otros algoritmos de encriptamiento existentes y sus principales características (complejidad, vulnerabilidad, áreas de aplicación, etc.).
- El alumno implementará en la computadora al menos uno de los algoritmos criptográficos revisados en clase.

# DE TEMA	TEMAS	INSTRUMENTACIÓN DIDÁCTICA	H/T	H/P	E.C.	CLAVE
7.1	**El algoritmo MD5.**	Exposición frente a grupo utilizando el pizarrón y acetatos.	1	1	1	1B, 2B
7.2	**El algoritmo SHA.**		1	1	1	
7.3	**El algoritmo IDEA.**	Realización de tareas y programas de computadora implementando algunos de los algoritmos de encriptamiento vistos en clase	1	1	1	
		Realización de prácticas de laboratorio.				
		SUBTOTAL	3	3	3	

No. UNIDAD: VIII **NOMBRE: AUTENTIFICACIÓN E INTERCAMBIO DE LLAVES**

OBJETIVOS PARTICULARES DE LA UNIDAD

- El alumno identificará los principales protocolos estándares para realizar autentificación en una red de comunicaciones de datos.
- El alumno analizará las principales características de dichos protocolos como lo son su complejidad, grado de seguridad que proporciona, requerimientos técnicos para su implementación en una red, funcionalidad proporcionada y principales aplicaciones de redes que lo utilizan.
- El alumno analizará algunos escenarios de sesión de una terminal que solicita algún servicio a un servidor utilizando una conexión con alguno de los protocolos de autentificación mencionados.

# DE TEMA	TEMAS	INSTRUMENTACIÓN DIDÁCTICA	H/T	H/P	E.C.	CLAVE
8.1	**Kerberos.** 8.1.1 Kerberos v4 y Kerberos v5. 8.1.2 Llaves privadas, de sesión y credenciales. 8.1.3 Escenario de autentificación en una sesión. 8.1.4 Software que corre sobre Kerberos.	Exposición frente a grupo utilizando el pizarrón y acetatos. Realización de tareas y programas por parte de los alumnos implementando algunas de las funciones de un protocolo de autentificación de datos.	2	2	2	1B, 2B
8.2	**X. 509: servicio de autentificación en directorios.**		1	2	2	
8.3	**Estándar para firmas digitales (DSS).**	Realización de prácticas de laboratorio.	1	1	2	
		SUBTOTAL	4	5	4	

No. UNIDAD: IX **NOMBRE: SEGURIDAD EN EL CORREO ELECTRÓNICO**

OBJETIVOS PARTICULARES DE LA UNIDAD

- El alumno evaluará y utilizará las principales recomendaciones y sistemas para la manipulación de mensajes de correo dentro de una red de comunicación de datos y sus características.
- El alumno analizará el grado de seguridad, privacidad e integridad que cada uno de los sistemas ofrece (soportado por los algoritmos de encriptamiento y autentificación previamente analizados), y comparará los sistemas de manejo de mensajes anteriores de acuerdo a sus características y determinará el sistema más adecuado de acuerdo a la aplicación y a la red que lo usará.
-

# DE TEMA	TEMAS	INSTRUMENTACIÓN DIDÁCTICA	H/T	H/P	E.C.	CLAVE
9.1	**Sistemas de manejo de mensajes (MHS).** 9.1.1 PGP. 9.1.2 PEM. 9.1.3 MOTIS (Message oriented Text Interchange System). 9.1.4 X.400 y X.420.	Exposición frente a grupo utilizando el pizarrón y acetatos. Realización de tareas y programas de computadora por parte de los alumnos implementando algunas de las funciones de uno o varios de los sistemas de manejo de mensajes vistos en clase. Realización de prácticas de laboratorio.	2	3	2	1B, 2B, 9C
		SUBTOTAL	2	3	2	

No. UNIDAD: X **NOMBRE: SEGURIDAD EN LA GESTIÓN DE REDES**

OBJETIVOS PARTICULARES DE LA UNIDAD

- El alumno identificará los principales protocolos de gestión de redes disponibles en la actualidad y analizará sus principales características, entre ellas su funcionalidad, complejidad y grado de seguridad e integridad de los datos transportados.

# DE TEMA	TEMAS	INSTRUMENTACIÓN DIDÁCTICA	H/T	H/P	E.C.	CLAVE
10.1	**Evolución de los Sistemas de Gestión de Redes.**	Exposición frente a grupo utilizando el pizarrón y acetatos.	1	0	1	2B, 8C, 10C
10.2	**SGMP (Simple Gateway Monitoring Protocol)**	Realización de tareas y programas de computadora por parte de los alumnos, implementando algunas de las funciones de un protocolo de gestión de red. Realización de prácticas de laboratorio.	1	2	1	
10.3	**SNMP y SNMPv2.** 10.3.1 MIB. 10.3.2 Seguridad.		1	3	1	
		SUBTOTAL	3	5	3	

# PRAC.	NOMBRE DE LA PRÁCTICA	RELACIONES DE U. TEMÁTICAS	HORAS PRAC.	LUGAR DE REALIZACIÓN
1	**Programación de encriptamiento por substitución ó por transposición.**	II	2	LABORATORIO DE COMPUTO
2	**Programación de encriptamiento por flujo ó por bloque.**	II	2	Y TELEMÁTICA
3	**Programa del estándar de encriptado de datos (DES).**	II	5	
4	**Programa del algoritmo Rivest-Shamir-Adleman (RSA).**	IV	5	
5	**Programa para encriptamiento con MD5, SHA ó IDEA.**	VII	3	
6	**Programa para autentificación: Kerberos ó firmas digitales (DSS).**	VIII	5	
7	**Programa para manejo de mensajes (MHS: PGP, PEM, MOTIS ó X.400).**	IX	3	
8	**Programa de un protocolo con funciones de seguridad utilizando alguno de los algoritmos anteriores.**	X	5	

PERIODO	UNIDADES TEMÁTICAS	PROCEDIMIENTOS DE EVALUACIÓN
1°	I, II, III, IV (4.1)	70% Examen departamental + 20% prácticas + 10% tareas.
2°	IV (4.2, 4.3), V, VI, VII	70% Examen departamental + 20% prácticas + 10% tareas.
3°	VIII, IX, X	70% Examen departamental + 20% prácticas + 10% tareas.

CLAVE	B	C	BIBLIOGRAFÍA
1	X		KAUFMAN, CHARLIE, PERLMAN, RADIA, SPECINER, MIKE, ***NETWORK SECURITY PRIVATE COMMUNICATION IN A PUBLIC WORLD***, 1° EDICIÓN, ED. PRENTICE HALL INC, PAG. 504, 1995
2	X		STALLINGS, WILLIAM, ***NETWORK AND INTERNETWORK SECURITY; PRINCIPLESN AND PRACTICE***, 1° EDICIÓN, ED. PRENTICE HALL
3	X		MEYER, CARL H., MATYAS, STEPHEN M., ***CRYPTOGRAPHY; A NEW DIMENSION IN COMPUTER DATA SECURITY***, 1° EDICIÓN, ED. JOHN WILEY AND SONS INC., PAG. 755, 1982
4		X	KONHEIM, ALAN G., ***CRYPTOGRAPHY A PRIMER***, 1° EDICIÓN, ED. JOHN WILEY AND SONS INC., PAG. 432, 1981
5		X	DEAVOURS, CIPHER A., KRUH LOUIS, ***MACHINE CRYPTOGRAPHY AND MODERN CRYPTANALYSIS***, 1° EDICIÓN, ED. ARTECH HOUSE INC., PAG. 259, 1985
6		X	KAHN, DAVID, ***THE CODEBREAKERS, THE STORY OF SECRET WRITING***, 1° EDICIÓN, ED. MACMILAN PUBLISHING CO., PAG. 1164, 1967
7		X	DAVIES, D. W., PRICE, W. L., ***SECURITY FOR COMPUTER NETWORKS***, 2° EDICIÓN, ED. JOHN WILEY AND SONS INC., PAG. 377, 1989
8		X	WILLIAM STALLINGS, ***SNMP, SNMPv2 AND CMIP; THE PRACTICAL GUIDE TO NETWORK MANAGEMENTS STANDARDS***, 1° EDICIÓN, ED. ADDISON WESLEY PUBLISHING CO., PAG. 625, 1993
9		X	PLATHER, B. C. LANZ, H. LUBICH, M. MÜLLER, T.WALTER, ***X 400 MESSAGE HANDLING, STANDARDS, INTERWORKING, APPLICATIONS*** , 1° EDICIÓN, ED. ADDISON WESLEY PUBLISHING CO., PAG. 378, 1991
10		X	UYLESS, BLACK, ***NETWORK MANAGEMENTSTANDARDS,. THE OSI, SNMP AND CMOL PROTOCOLS***, 1° EDICIÓN, ED. MC. GRAW HILL INC., PAG. 336, 1992