UNIVERSIDAD NACIONAL DE CÓRDOBA
Facultad de Ciencias Exactas, Físicas y Naturales
República Argentina

Programa de:

Criptografía y Seguridad en Redes

Código: **2645**

Carrera: *Ingeniería en Computación*	Plan:	*285-05*	Puntos:	*4*
Escuela: *Ingeniería Computación*.	Carga Horaria:	*72*	Hs. Semanales:	*4,5*
Departamento: *Computación.*	Semestre:	*Segundo*	Año:	*Quinto*
	Carácter:	*Selectiva*		

Objetivos:

Capacitar al alumno en el área de seguridad informática para que pueda:

- *Identificar aspectos fundamentales de la criptografía simétrica y asimétrica, y sus aplicaciones.-*
- *Utilizar la criptografía simétrica y asimétrica para implementar servicios de confidencialidad, integridad, autenticación y no repudio.*
- *Integrar en sus proyectos los principales métodos y protocolos utilizados en la implementación servicios de seguridad en internet.-*

Programa Sintético:

Capítulo 1: Conceptos Básicos de Seguridad Informática
Capítulo 2: Criptoalgorítmos Clásico
Capítulo 3: Criptoalgoritmos de clave pública
Capítulo 4: Servicios de Seguridad; Firma Digital.
Capítulo 5: Administración de claves.
Capítulo 6: Estándares criptográficos y protocolos seguros para Internet.
Capítulos 7: Criptografía cuántica y computación cuántica.

Programa Analítico: de foja *2* a foja *2*.

Programa Combinado de Examen (si corresponde): de foja a foja .

Bibliografía: de foja *3* a foja *3*.

Correlativas Obligatorias:
1. *Algoritmos y Estructuras de Datos.*
2. *Comunicaciones de Datos.*

Correlativas Aconsejadas:

Rige: *2005*

Aprobado HCD, Res.:	Modificado / Anulado /Sust. HCD Res.:
Fecha:	Fecha:

El Secretario Académico de la Facultad de Ciencias Exactas, Físicas y Naturales (UNC) certifica que el programa está aprobado por el (los) número(s) y fecha(s) que anteceden. Córdoba, / / .

Carece de validez sin la certificación de la Decretaría Académica:

PROGRAMA ANALITICO

LINEAMIENTOS GENERALES

Criptografía y Seguridad en Redes es una actividad curricular selectiva y exclusiva para los estudiantes de Ingeniería en Computación.

La materia es una introducción al tema de criptografía, sus aplicaciones en los servicios de seguridad como confidencialidad, integridad y autenticación. Luego, estos servicios básicos se integran en mecanismos más complejos de seguridad, como protocolos, para brindar servicios al tráfico de información en redes de computadoras.

A partir del estudio de la criptografía es posible definir mecanismos que permitan brindar servicios integrales más complejos como la firma electrónica, el intercambio de claves y el soporte para el comercio electrónico seguro sobre una red insegura como Internet.

En esta era de conectividad electrónica global, de virus y hackers, de escuchas y fraude electrónico, no hay aspecto en donde la seguridad no importe. En un intento de simplificar, podemos decir que dos puntos han hecho a los contenidos de esta materia de vital interés: **Uno**, el explosivo crecimiento de los sistemas de computadoras y su interconexión mediante redes ha incrementado la interdependencia de organizaciones e individuos del almacenamiento y transmisión de la información utilizando estos sistemas. Esto ha llevado al interés de proteger los datos y los recursos que le dan soporte para garantizar un nivel de seguridad mínimo. **Segundo**, tanto la criptografía como de la seguridad en redes han madurado, conduciendo al desarrollo de aplicaciones que permiten forzar la seguridad en las redes de computadoras, tales como Internet.

METODOLOGIA DE ENSEÑANZA

Los alumnos asisten a clases teóricas y prácticas, a cargo del Profesor Adjunto a cargo de la Cátedra.
Las actividades teóricas se realizan mediante exposiciones del docente orientadas a presentarle al estudiante los aspectos teóricos que fundamentan las técnicas y metodologías que se aplicarán en la resolución de problemas y en las prácticas de laboratorio.
Las clases prácticas se orientan a dos tipos de actividades; la resolución de problemas y clases de laboratorio en las que se realizan implementaciones reales y virtuales. Es en este último tipo de actividad en donde se alcanza el mayor impacto, en lo que a metodología de aprendizaje se refiere. La experiencia de laboratorio se revela como una herramienta insustituible para afianzar los contenidos vertidos tanto en las clases teóricas, como en la resolución de problemas.
El Laboratorio de Computación provee del espacio para el dictado de los teóricos y en el año 2010, a través del Laboratorio de Redes, y un convenio con Cisco, se recibió la donación de hardware y software para llevar adelante las prácticas de en seguridad en redes.
Desde el año 2007 los contenidos teóricos de la materia se encuentran disponibles para los alumnos en un aula virtual implementada con moodle.

EVALUACION

Condiciones para la promoción de la materia

1. Tener aprobadas las materias correlativas.
2. Asistir al 80% de las clases teóricas y prácticas.
3. Aprobar dos exámenes parciales con nota no inferior a seis (6). En los parciales se evalúan tanto la capacidad para resolver problemas, como los conocimientos de los contenidos teóricos de la materia.
4. Aprobar la totalidad de los trabajos de Laboratorio.
5. Aprobar un coloquio integrador.

Los alumnos que cumplan con el 50% de las exigencias referidas a los parciales y trabajos de Laboratorio y tengan la asistencia requerida en el punto dos serán considerados Alumnos Regulares, el resto se considerarán Alumnos Libres.

CONTENIDOS TEMATICOS

Capítulo 1: Conceptos Básicos

La necesidad de servicios de seguridad en las redes actuales.
Riesgos de la seguridad en computadoras. Servicios de seguridad en redes de computadoras y otros elementos presentes en una red: confidencialidad, integridad, autenticación, no rechazo, identificación, control de acceso, auditabilidad. Comercio electrónico y otras aplicaciones de los servicios de seguridad en las redes actuales. Reconocimiento de servicios de encripción comunes y extraordinarios. Los diez mandamiento de Shamir para la seguridad comercial.

Conceptos básicos de criptografía.
Criptosistema, texto plano, texto cifrado, clave. Ejemplos de criptosistemas simples. Publicar o no publicar ?. Investigaciones secretas y públicas sobre criptografía. Implementaciones de hardware vs implementaciones de software. Evolución de la criptografía y el criptoanálisis.

Tipos de criptosistemas. Implementación de servicios de seguridad.
Criptosistemas clásicos (simétricos) y de clave pública (asimétricos). Principales componentes de un criptosistema de clave pública. Requerimientos para la cifra de hoy en día. Implementaciones de servicios de seguridad usando transformaciones criptográficas. Cifra de bloques vs cifra de cadenas. Medición de la fortaleza de una cifra.

Capítulo 2: Criptoalgorítmos Clásicos

Revisión de la historia de la cifra.
Cifra de sustitución: Monoalfabética. Polialfabética. Distribución de claves. Poligramas. Homofónica. Cifra de transposición. Ruptura mediante el uso del análisis de frecuencia. Teoría de Shanon del secreto perfecto y sus aplicaciones prácticas. Data Encryption Standard – primer intento de estandarizar la protección de la información en redes de computadoras.

Revisión histórica de los criptosistemas
Los roles de NBS – NSA – IBM. Aceptación por parte de organismos oficiales y sectores comerciales. Principales características del algoritmo. Criterios de diseño. Criptoanálisis diferencial y lineal. Vulnerabilidad a un ataque de búsqueda exhaustiva de clave. Triple DES: Modos de operación. Seguridad de los diferentes modos de operación.

Otras cifras de bloque de clave simétrica.
IDEA, RC5, Blowfish, DESX, Skipjack. Algoritmos de cifrado para una implementación rápida por software.

Implementación de cifras de bloque de clave secreta
Arquitecturas generales de hardware y software. Implementaciones básicas, operación de los componentes de software y hardware. Arquitecturas de fast-hardware: loop unrolling; inner-round pipelining; outer-round pipelining; mixed inner- and outer-round pipelining. Limitaciones impuestas por el ambiente de implementación.

Desarrollos de nuevo Advanced Encryption Standard –AES.
Contexto de desarrollo. Criterios de evaluación. Algoritmos candidatos a AES. Comparación de los candidatos a AES: Seguridad; Eficiencia en la implementación por software; Eficiencia en la implementación por hardware; Flexibilidad; Procesos de evaluación.

Capítulo 3: Criptoalgoritmos de clave pública.
Criptosistemas RSA (Rivest, Shamir, Adleman) – el primer criptosistema de clave pública exitoso.
Cómo se gestó RSA. RSA como una función de una sola vía con "trapdoor". La factorización como principio de seguridad en RSA: registro de factorización; factorización de grandes números mediante el uso de redes distribuidas de computadoras. Desafíos de RSA. Tamaños de clave recomendados en los criptosistemas RSA.

Generación de claves en los criptosistemas RSA.
Propósitos generales vs propósitos especiales en los algoritmos de factorización. RSA para paranoicos. Fortaleza de los números primos. Test probabilístico para detectar primos. Test determinístico para detectar primos. Construcción de números primos grandes y randómicos.

Implementación de cifrado de clave pública.
Algoritmos de exponenciación básicos. Uso del teorema de los restos chinos para una rápida exponenciación. Algoritmos básicos para multiplicación y reducción modular por software. Arquitecturas básicas para multiplicación y reducción modular por hardware. Dependencia entre la longitud de clave y el tiempo de transformación criptográfica. Reconocimiento de implementaciones existentes de RSA.

Capítulo 4: Servicios de Seguridad
Firma Digital. Digital Signature Standard – DSS.
Clasificación de firmas digitales. Ataques contra la firma digital. Relleno de seguridad para firmas. Digital Signature Standard (DSS). Análisis comparativo de RSA y DSS – Seguridad, perfomance, funcionalidad. Temas legales respecto a la firma digital.

Integridad de datos y autenticación – dos faces del mismo problema. Funciones de hash y MACs.
Requerimientos para una función de hashing segura. Clasificación de las funciones de hashing. Ataques contra funciones de hashing. Aplicaciones estándar y no estándar.: firma digital y códigos de autenticación; detección de virus; almacenamiento de password; cifrado rápido. Familias de algoritmos para funciones de hashing y su seguridad. Requerimientos para Message Authentication Code (MAC). Familias de MACs y su seguridad. Combinación de autenticación y confidencialidad.

Capítulo 5: Administración de claves
Intercambio de claves para criptosistemas de clave simétrica.
Clave de sesión y clave de encripción. Intercabio de claves usando centros de distribución. Protocolo de intercambio de clave de Diffie-Hellman. Intercambio de claves simétricas utilizando criptosistemas de clave pública.

Certificados de clave pública e infraestructuras de autoridades de certificación. Generación y registro del par de claves públicas. Concepto de certificado de clave pública. Formatos de los certificados (X.509; EDIFACT; etc.). Estructura jerárquica y autoridades de certificación en una estructura de clave pública. Revocación de certificados.

Capítulo 6: Estándares criptográficos y protocolos seguros para Internet.
Estándares critptográficos de USA y resto del mundo.
Organizaciones que administran estándares. Principales grupos de estándares criptográficos: Estándares federales (USA); Estándares ANSI; Estándares del IEEE; Estándares ISO; Estándares informales de la industria. Estándares para la criptografía clásica. Estándares para la criptografía de clave pública.

Protocolos seguros para Internet.
Correo electrónico seguro: S/MIME; Open PGP. Web Site seguros: SSL; S-HTTP. Protocolos de seguridad para pagos con tarjeta: SET; dinero electrónico; micropagos. Redes privadas virtuales seguras: IPSec; PPTP. Controles de importación y exportación de dispositivos criptográficos. Evolución de las políticas de USA. Reglamentación actual en USA.

Capítulos 7: Criptografía cuántica y computación cuántica
Criptografía cuántica – Criptografía para el siglo XXI ..?
Conceptos básicos de la criptografía cuántica – traslado del principio de Hisenberg para una seguridad ideal. Primeras implementaciones prácticas de la criptografía cuántica – perfomance; costos; actuales limitaciones. Hacia una computación cuántica. Ruptura de cifras usando la computación cuántica – sueño o realidad .?. Reemplazará la física a la matemática como la base para el desarrollo de la seguridad en redes de computadoras.?. Tendencia de las corrientes investigaciones en criptografía, seguridad en redes y el desarrollo de software seguro.

LISTADO DE ACTIVIDADES PRACTICAS Y/O DE LABORATORIO

Actividades Prácticas

1. **Propiedades de los criptosistemas de clave secreta**
   - Propiedades de los criptosistemas DES.
   - Generación de claves.
   - Longitud del texto después del cifrado y después del descifrado.
   - Tiempo de cifrado y tiempo de descifrado.
   - Seguridad en los distintos modos de operación.
   - Resistencia a los errores de transmisión.
   - Claves débiles.
   - Efectos de cambiar un simple bit de una clave DES.

2. **Propiedades de los criptosistemas de clave pública**
   - Propiedades de los criptosistemas RSA
   - Generación y almacenamiento de claves.
   - Longitud del mensaje despues del cifrado.
   - Tiempo de cifrado y descifrado para exponentes de clave pública y privada de igual longitud.
   - Elección de un exponente para la clave pública y su influencia en los tiempos de cifrado y descifrado.
   - Resistencia a los errores de transmisión.

- Comparación de las velocidades para DES y RSA en sus implementaciones de software.
- Transmisión de claves para DES.

3. Implementación de la seguridad en Redes

- Armado, configuración y puesta en marcha de diferentes escenarios para asegurar el tráfico de información en redes de computadoras.

DISTRIBUCION DE LA CARGA HORARIA

ACTIVIDAD	HORAS
TEÓRICA	42
FORMACIÓN PRACTICA:	
o FORMACIÓN EXPERIMENTAL	8
o RESOLUCIÓN DE PROBLEMAS	12
o ACTIVIDADES DE PROYECTO Y DISEÑO	10
o PPS	
TOTAL DE LA CARGA HORARIA	72

DEDICADAS POR EL ALUMNO FUERA DE CLASE

ACTIVIDAD		HORAS
PREPARACION TEÓRICA		42
PREPARACION PRACTICA		
	o EXPERIMENTAL DE LABORATORIO	8
	o EXPERIMENTAL DE CAMPO	
	o RESOLUCIÓN DE PROBLEMAS	12
	o PROYECTO Y DISEÑO	10
	TOTAL DE LA CARGA HORARIA	72

BIBLIOGRAFIA

Principal:

1. William Stallings, Cryptography and Network Security: Principles and Practice, 2nd ed., Prentice Hall, 1999.

Opcional:

1. Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, Inc., Boca Raton, 1996 (Todos los capítulos de este libro pueden ser bajados del web site del libro).
2. Bruce Schneier, Applied Cryptography - Protocols, Algorithms, and Source Code in C, 2nd ed., John Wiley & Sons, Inc., New York, 1995.
3. Recursos matemáticos básicos relacionados Capítulo 7 de William Stallings, Cryptography and Network Security: Principles and Practice, 2nd ed., Prentice Hall, 1999.
4. Capítulo 2 y 4 de Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, Inc., Boca Raton, 1996.
5. Recursos matemáticos intermedios relacionados David M. Burton, Elementary Number Theory, International Series in Pure and Applied Mathematics, 3rd. ed., The McGraw-Hill Companies, Inc., 1997.
6. Neal Koblitz, A Course in Number Theory and Cryptography, 2nd ed., Springer-Verlag, New York, 1994.

Lecturas adicionales

1. Aviel D. Rubin, Daniel Geer, and Marcus J. Ranum, Web Security Sourcebook: A Complete Guide to Web Security Threats and Solutions, John Wiley & Sons, Inc., 1997.
2. Douglas R. Stinson, Cryptography - Theory and Practice, CRC Press, Inc., Boca Raton, 1995.
3. Charlie Kaufman, Radia Perlman, and Mike Speciner, Network Security: Private Communication in a Public World, PTR Prentice Hall, Englewood Cliffs, 1995.
4. Bruce Schneier, E-mail Security: How to Keep Your Electronic Messages Private, John Wiley & Sons, Inc., 1995.
5. Gregory B. White, Eric A. Fisch, and Udo W. Pooch, Computer System and Network Security, CRC Press, Inc., Boca Raton, 1996.
6. Brent Chapman and Elizabeth D. Zwicky, Building Internet Firewalls, O'Reilly & Associates, Inc., Sebastopol, 1995.
7. William R. Cheswick, Steven M. Bellovin, Firewalls and Internet Security: Repelling the Wily Hacker, Addison-Wesley Publishing Company, 1994.