CARRERA	ASIGNATURA	Año	Régimen[1]	Plan	Total Horas
Ingeniería en Sistemas	Criptografía y Seguridad Informática	5to	2do Cuatr.	072/08	60

EQUIPO DOCENTE:

PROFESOR	CATEGORÍA
	Titular
	Asociado
CURTI, Hugo Javier	Adjunto
	Jefe de Trabajos Prácticos
	Ayudante de 1ª
	Ayudante de 2da

1. CONTENIDOS MÍNIMOS[2]:

Historia de la criptografía. Criptografía Clásica, Moderna: de clave Secreta – Simétrica y de clave Pública – Asimétrica. Protocolos TLS/Kerberos/IPSec. Redes Wireless. Funciones hash Criptográficas. Certificados Digitales y Firmas. Introducción a las Curvas Elípticas. Introducción a la Criptografía Quántica. Virus informático: antivirus y contramedidas. Actividad de intrusos. Comunicación segura. Seguridad física. Seguridad en redes y criptografía aplicada en redes.

2. CONTENIDOS DE LA ASIGNATURA[3]:

Unidad Nº 1 - Conceptos básicos de Seguridad:

Contenidos:

Definición de seguridad. Principios de seguridad: integridad, confidencialidad, disponibilidad, irrefutabilidad. Seguridad por oscuridad y exposición. Seguridad Paranoica. Falsa Seguridad. Definición de conceptos empleados en seguridad: vulnerabilidad, riesgo, ataque, impacto. Seguridad precavida, reactiva y proactiva. Ingeniería Social. Técnicas para incrementar la seguridad: criptología, criptografía, criptoanálisis, esteganografía, esteganoanálisis.

Unidad Nº 2 - Criptología:

Contenidos:

Definición de criptología, criptografía, criptoanálisis, esteganografía y esteganoanálisis. Conceptos utilizados en criptología: criptosistema, criptograma, mensaje en claro, clave, codificación y decodificación, cifrado y descifrado.

Unidad Nº 3 - Criptografía Antigua:

Contenidos:

Historia de la criptografía: utilización en la Edad Media, Segunda Guerra Mundial, Guerra Fría, Actualidad. Cifrados clásicos: sustitución y transposición. El cifrado de César, sustitución monoalfabética y polialfabética. Sustitución homofónica. Cifrado de *Vigenère*. La máquina Enigma.

Unidad Nº 4 - Criptografía Moderna:

Contenidos:

Criptografía simétrica de una y dos vías. Base matemática de la criptografía simétrica.

1 Anual, Primer Cuatrimestre ó Segundo Cuatrimestre

2 Se deberán consignar los mismos, tal como se encuentran aprobados en el Plan de Estudios aprobado por Resolución Rectoral.

3 Cada Unidad Temática estará identificada por un nombre que describa claramente una unidad de conocimientos coherentes, la descripción de los mismos, la bibliografía especifica para la misma (puede ser la misma en varias unidades o tener cada una de ellas diferencias con otras) y la manera en que serán evaluados esos contenidos.

Algoritmos criptográficos de una vía: *Secure Hash Algorithm* (SHA), *Message Digest Algorithm* 5 (MD5). Algoritmos criptográficos de dos vías: *Data Encryption Standard* (DES), Triple DES (TDES), *Advanced Encryption Standard* (AES). Criptografía asimétrica. Fundamentos. Utilización para autenticar, cifrar, firmar y garantizar irrefutabilidad. Base matemática de la criptografía asimétrica. Algoritmo: RSA. Criptografía de Curva Elíptica (ECC): *Digital Signature Algorithm* (DSA). Introducción a la Criptografía Cuántica.

Unidad Nº 5 - Criptoanálisis:

Contenidos:

Técnicas de criptoanálisis. Análisis de la frecuencia. Índice de coincidencia. Criptoanálisis lineal, diferencial, integral, de módulo n, estadístico, XSL. Ataques criptoanalíticos: deslizamiento, *birthday*, *man-in-the-middle*, *meet-in-the-middle*, fuerza bruta, clave relacionada.

Unidad Nº 6 - Software Criptográfico:

Contenidos:

PGP/GPG. Historia. Modelo de redes de confianza. Utilización práctica. Estándar X-509. Autoridades Certificantes. Infraestructura de Claves Públicas (PKI). *OpenSSL*. Generación de Certificados. Protección de Contraseñas. Estándar SASL. Implementaciones de SASL.

Unidad Nº 7 - Ataque y defensa de Sistemas Informáticos:

Contenidos:

Análisis y descripción de las amenazas actuales. Definición de términos: *Malware*, *Spyware*, Virus, Gusano, Troyano, SPAM. Vulnerabilidades: saturación de memoria, ejecución de código arbitrario, escalamiento de privilegios, *cross-site scripting*, inyección de código SQL, liberación de información (*disclosure*). Herramientas de defensa y ataque: capturadores de paquetes, escaneadores de puertos, *rootkits*, escaneadores de vulnerabilidades. Ataques contra sistemas y redes o usuarios de los mismos: SCAM, *BlueJack*, *Phishing*, ataques de negación de servicio (DoS), DoS distribuidos (DDoS), espionaje de redes inalámbricas. Ataques dirigidos. Fraudes. Vandalismo Informático. Terrorismo Informático. Términos con que se definen actores de la Seguridad Informática: *Hacker* y sus acepciones, *Cracker*, *Script Kiddie*.

Unidad Nº 8 - Normas y Organismos de Seguridad Informática:

Contenidos:

Introducción a las políticas de Seguridad. Función de las políticas de seguridad en una organización. Creación de políticas de seguridad. Norma ISO / IEC 27002 (ex 17799). Ley Orgánica de Protección de Datos de Carácter Personal (España). Organismos Oficiales de Seguridad CERT / ARCERT.

3. PROGRAMA DE TRABAJOS PRÁCTICOS[4]:

Práctico Nº 1 – Conceptos básicos de Seguridad

Objetivo:

Fijar mediante ejercitación los conceptos básicos de seguridad.

Actividades a desarrollar:

Sobre papel y lápiz se analiza la seguridad de diferentes sistemas a partir de narrativas, se solicita al estudiante que plantee nuevos escenarios y que busque ejemplos de los diferentes conceptos estudiados.

4 Cada Trabajo Práctico estará identificada por un nombre que describa claramente una finalidad coherente de ejecución; las actividades que se desarrollaran (realización de ejercicios teóricos, practicas de laboratorio, etc.); y un listado de materiales o de elementos necesarios para su ejecución, si fuera del caso (reactivos, guías de problemas, instrumentos, hardware especifico, software a utilizarse, etc.).

Materiales:
Guía de trabajos prácticos, lápiz y papel.

Práctico Nº 2 - Criptografía

Objetivo:
Fijar mediante ejercitación los conceptos y técnicas de criptografía antigua aprendidos.

Actividades a desarrollar:
Aplicar algoritmos criptográficos clásicos, junto con las claves correspondientes, para recuperar un mensaje cifrado.
Materiales:
Guía de trabajos prácticos, lápiz y papel.

Práctico Nº 3 - Criptoanálisis

Objetivo:
Fijar mediante ejercitación los conceptos y técnicas de criptoanálisis clásico aprendidos.

Actividades a desarrollar:
Criptoanalizar textos cifrados y obtener su contenido. Esta vez por ser práctica de criptoanálisis se hace sin las claves.
Materiales:
Guía de trabajos prácticos, lápiz y papel.

Práctico Nº 4 – Criptografía Simétrica

Objetivo:
Fijar mediante ejercitación los conceptos y técnicas de criptografía simétrica moderna aprendidos.

Actividades a desarrollar:
Probar los conceptos aprendidos mediante una actividad guiada utilizando herramientas criptográficas de software libre.
Materiales:
Guía de trabajos prácticos, lápiz, papel, computadora personal o portátil, Distribución de GNU/Linux básica con el software GNUPG instalada o en medio extraíble.

Práctico Nº 5 – Criptografía Asimétrica

Objetivo:
Fijar mediante ejercitación los conceptos y técnicas de criptografía asimétrica moderna aprendidos.

Actividades a desarrollar:
Probar los conceptos aprendidos mediante una actividad guiada utilizando matemática simple y luego herramientas criptográficas de software libre.
Materiales:
Guía de trabajos prácticos, lápiz, papel, computadora personal o portátil, Distribución de GNU/Linux básica con el software GNUPG instalada o en medio extraíble.

Práctico Nº 6 – GPG y X509

Objetivo:
Aprender a utilizar el software GNUPG (GPG) y fijar mediante ejercitación los conceptos que incumben al protocolo X509.

Actividades a desarrollar:
Probar los conceptos aprendidos mediante una actividad guiada utilizando herramientas criptográficas de software libre.

Materiales:
Guía de trabajos prácticos, lápiz, papel, computadora personal o portátil, Distribución de GNU/Linux básica con el software GNUPG y el

software OpenSSL instalada o en medio extraíble.

4. BIBLIOGRAFÍA[5]:

BIBLIOGRAFÍA BÁSICA			
TITULO	**AUTOR(ES)**	**EDITORIAL**	**LUGAR Y AÑO DE EDICIÓN**
RFC 5280: Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile	Cooper D.; Santesson S.; Farrel S.; S.Boeyen; Housley R.; Polk W.	Internet Engineering Task Force (IETF)	2008
RFC 4880: OpenPGP message format	Callas J.; Donnerhacke L.; Finney H.; Shaw D.; Thayer R.	Internet Engineering Task Force (IETF)	2007
ISO/IEC 27002: Information technology - security techniques - code of practice for informa-tion security management	-	International Organization for Standardization and International Electrotechnical Commission.	2006
Beyond Fear: Thinking Sensibly about Security in an Uncertain World	Schneier B.	Springer-Verlag New York, Inc.	2003
Secrets & Lies: Digital Security in a Networked World	Schneier B.	John Wiley & Sons, Inc.	2000
Self-study course in block cipher cryptanalysis	Schneier B.	En Cryptologia, tomo 24(1):págs. 18–34. http://www.schneier.com/paper-self-study.pdf.	2000
RFC 2510: Internet X.509 public key infrastructure certificate management protocols	Adams C.; Farrell S.	Internet Engineering Task Force (IETF)	1999
Ley orgánica 15/1999, de protección de datos de carácter personal	-	Boletín Oficial del Estado Español Nro. 298 páginas 43088-43099	1999
The Official PGP User's Guide	Zimmermann P. R.	The MIT Press	1995
Differential cryptanalysis of DES-like cryptosystems	Biham E.; Shamir A.	Journal of Cryptology, tomo 4(1):páginas 3–72 (1991)	1991
A method for obtaining digital signatures and public- key cryptosystems	Rivest R.; Shamir A.; Adleman L.	Communications of the ACM, tomo 21(2):páginas 120–126 http://theory.lcs.mit.edu/rivest/rsapaper.pdf	1978
The Mathematical Theory of Communication	Shannon C.; Weaver W.	University of Illinois Press	1963

NECOCHEA, Provincia de Buenos Aires, 12 de Julio de 2017.

Profesor Titular

5 Se requiere consultar en la Biblioteca de la UNdeC la existencia de textos referidos a la temática de cada asignatura a fin de trabajar con material ya existente, en caso de no existir textos relacionados realizar la solicitud correspondiente.