

TEORÍA DE LA INFORMACIÓN Y CRIPTOGRAFÍA BÁSICA

Curso 2013/2014

(Código:71024091)

1. PRESENTACIÓN DE LA ASIGNATURA

Esta guía presenta las orientaciones básicas que se requieren para el estudio de la asignatura de *Teoría de la información y criptografía básica*. Por esta razón se recomienda leer detenidamente esta guía antes de iniciar el estudio, con el objetivo de hacerse una idea general de la asignatura y de los trabajos, actividades y prácticas que se van a desarrollar a lo largo del curso.

Teoría de la información y criptografía básica es una asignatura de seis créditos ECTS de carácter optativo que se imparte en el primer semestre del cuarto curso de carrera en la titulación de Grado en Ingeniería en Tecnologías de la Información dentro de la materia de *Seguridad y Auditoría de la Información*.

El objetivo esencial de la asignatura es adquirir los conocimientos fundamentales asociados a la teoría de la información y la criptografía, orientándolos a la comprensión de las técnicas y su implantación en proyectos tecnológicos. En este sentido, se analizan las propiedades de la información, los procedimientos de cifrado y sus aplicaciones prácticas.

2. CONTEXTUALIZACIÓN EN EL PLAN DE ESTUDIOS

La asignatura de *Teoría de la información y criptografía básica* se encuadra en la materia de *Seguridad y Auditoría de la Información*. Esta misma materia se compone además de otras dos asignaturas estrechamente relacionadas:

- *Procesamiento y herramientas de gestión de la seguridad de redes*, asignatura obligatoria del primer semestre de tercer curso.
- *Consultoría y auditoría*, que se cursa de forma optativa en el segundo semestre del tercer curso.

Esta asignatura es asimismo una extensión de la asignatura de *Seguridad*, que se imparte en tercer curso de la Ingeniería en Informática.

Las competencias educativas atribuidas a la asignatura de *Teoría de la información y criptografía básica* participan del conjunto de competencias de la materia en *Seguridad y Auditoría*. Específicamente la asignatura contribuye al desarrollo de las siguientes competencias generales y específicas, que son comunes a los dos grados en que se imparten.

Las competencias genéricas se articulan en cuatro áreas competenciales y recogen los tres niveles especificados en los Descriptores de Dublín. En cuanto a la asignatura de *Teoría de información y criptografía básica* se concreta en:

- *Competencias cognitivas superiores*(G.2): selección y manejo adecuado de conocimientos, recursos y estrategias cognitivas de nivel superior apropiados para el afrontamiento y resolución de diversos tipos de tareas/problemas con distinto nivel de complejidad y novedad: Análisis y Síntesis. Aplicación de los conocimientos a la práctica Resolución de problemas en entornos nuevos o poco conocidos. Pensamiento creativo. Razonamiento crítico. Toma de decisiones.
- *Competencias en el uso de las herramientas y recursos de la Sociedad del Conocimiento*(G.5): Manejo de las TIC. Competencia en la búsqueda de información relevante. Competencia en la gestión y organización de la información.



Competencia en la recolección de datos, el manejo de bases de datos y su presentación

- *Trabajo en equipo*(G.6). Trabajo en equipo desarrollando distinto tipo de funciones o roles. En la Sociedad del Conocimiento se presta especial atención a las potencialidades del trabajo en equipo y a la construcción conjunta de conocimiento, por lo que las competencias relacionadas con el trabajo colaborativo son particularmente relevantes.

En cuanto a las competencias específicas, se concreta para la asignatura de *Teoría de la información y criptografía básica*, las propias del bloque Común a la Rama de Informática y las del bloque específico de las Tecnologías de la Información.

- Conocimiento y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos. (BC.6)
- Capacidad de comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos. (BTeti.7)

Asimismo la asignatura concreta otras competencias recomendadas para títulos en la rama informática:

- Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido.
- Capacidad para comprender y poder aplicar conocimientos avanzados de computación de altas prestaciones y métodos numéricos o computacionales a problemas de ingeniería.

La intensificación en la materia requiere un nivel medio, en algunas competencias medio-alto, para alcanzar un nivel considerado suficiente para poder participar con éxito en el ámbito de la seguridad, como elemento importante en los proyectos de ingeniería informática.

3.REQUISITOS PREVIOS REQUERIDOS PARA CURSAR LA ASIGNATURA

Esta asignatura requiere de un conocimiento básico y las competencias adquiridas en materias cursadas previamente, como las relacionadas con redes, así como con lenguajes de programación. Asimismo requiere de los conocimientos de la asignatura obligatoria de la materia de Seguridad de tercer curso.

4.RESULTADOS DE APRENDIZAJE

El objetivo básico de la asignatura es dar una visión completa de los fundamentos básicos de la teoría de la información y la criptografía. Como resultado del estudio y aprendizaje de los contenidos de esta asignatura el alumnado será capaz de:

- Comprender las técnicas básicas sobre los procedimientos de difuminación de la información mediante cifrado mediante una revisión histórica de los diferentes métodos empleados hasta nuestro tiempo (RA4). Está relacionado con las competencias genéricas G.2 y específicas BC.6 mencionadas anteriormente.
- Analizar el funcionamiento de los algoritmos de secreto compartido (clave privada) y cifrado público, y las implicaciones más importantes de su utilización como por ejemplo la distribución segura de la clave compartida (RA5). Está relacionado con las competencias genéricas G.2, G.5, y específicas BC.6, BC.6, BTeti.7.
- Desarrollar proyectos de uso de las técnicas criptográficas mediante la arquitectura de seguridad criptográfica de Java e implementar procedimientos de seguridad basadas en los algoritmos criptográficos más comunes (RA7). Relacionado con las competencias generales G.5, G.6 y específicas BC.6, BTeti.7.



5.CONTENIDOS DE LA ASIGNATURA

Los contenidos de la asignatura se distribuyen en tres módulos.

Módulo I. Teoría de la Información.

Este bloque temático permite introducir al estudiante en uno de los pilares básicos de la ingeniería de la seguridad de los sistemas de información, presentándolo como una progresión en el conocimiento matemático-científico.

- Unidad 1. Introducción a la criptología.
 - Introducción, conceptos y definiciones.
 - El modelo de seguridad: triángulo CIA en criptología.
 - Sustitución y transposición.
 - El principio de Kerckhoffs.
 - Funciones de una vía.
 - La generación de números aleatorios.
 - En flujo o en bloque.
 - Otras disciplinas relacionadas: esteganografía y su utilidad.
- Unidad 2. Procedimientos clásicos de cifrado
 - Los primeros cifrados conocidos.
 - Procedimientos clásicos por sustitución. El caso del César.
 - Procedimientos clásicos por transposición. La escítala.
 - Sistemas criptográficos medievales y modernos.
 - Criptografía en los conflictos y en la diplomacia.
- Unidad 3. Introducción al Criptoanálisis
 - Introducción al criptoanálisis.
 - Criptoanálisis y hacking ético.
 - Taxonomía de ataques
 - Espacio de claves y debilidad.
 - Ataque por fuerza bruta.
 - Ataques estadísticos.
 - Otras técnicas emergentes.
- Unidad 4. Teoría de la Información
 - Introducción.
 - Probabilidad y eventos independientes.
 - La teoría de Shannon.



- Confusión y difusión.
- Entropía y métricas de la información.
- El concepto de secreto perfecto.
- La cifra de Vernam.

■ Unidad 5. Distribución de las letras de una lengua escrita

- Introducción.
- Estudio estadístico de letras.
- Entropía de una lengua. Absoluta y relativa a un mensaje.
- Bigramas y trigramas. N-gramas.
- Modelos de lenguaje: Trabajos relacionados de PLN.

Módulo II. Criptografía y tipos de algoritmos: Protocolos criptográficos y firmas digitales.

Este módulo forma la parte central de la asignatura y consiste en el estudio principal sobre la criptografía de clave privada y la criptografía de clave pública. Entre las aplicaciones más importantes describiremos la firma digital.

■ Unidad 6. Criptografía de Clave Privada.

- Sistemas simétricos. En flujo y en bloque.
- Fundamentos del cifrado en bloque.
- Modos de operación.
- Sustituciones y permutaciones. Cifradores iterativos.
- Cifradores de Feistel. El algoritmo DES.
- El estándar AES. La propuesta de Rijndael.
- El cifrado de disco. XTS-AES.
- Otros algoritmos: IDEA, Blowfish, RC5.

■ Unidad 7. Criptografía de Clave Pública.

- Conceptos de los sistemas asimétricos.
- El algoritmo RSA.
- El algoritmo de El Gamal.
- Otras cifras asimétricas: ECC, Rabin.

■ Unidad 8. Protocolos criptográficos y firmas digitales.

- El protocolo híbrido del sobre digital.
- Esquema de firma digital. El estándar de firma DSA.
- La firma RSA.
- La firma El Gamal.



- Otros protocolos de firma: ECDSA, de Rabin.
- La familia PKCS .
- Protocolos de verificación de la firma. El ISO 9796.

Módulo III. Aplicaciones prácticas de la criptografía.

Este módulo consiste en el estudio de las aplicaciones criptográficas que se realizan en los sistemas diseñados de la industria de las tecnologías. Es el caso de la autenticación de mensajes, la identificación de entidades o usuarios, la seguridad aplicada a la web, el correo electrónico seguro, las aplicaciones bancarias y el comercio electrónico.

- Unidad 9. Autenticación de un mensaje.
 - Introducción. Integridad de datos.
 - Funciones Hash. Clasificación.
 - Propiedades y modelo general.
 - Hash sin clave. MD5, SHA.
 - Hash autenticado. MAC.
 - Algoritmos de autenticación de mensajes. MD5-MAC
- Unidad 10. Identificación del usuario.
 - Esquemas de identificación.
 - Autenticación débil: contraseñas.
 - Contraseña de un solo uso: OTP.
 - Autenticación fuerte: protocolos de desafío-respuesta.
 - Protocolos basados en ZK o conocimiento cero.
- Unidad 11. Seguridad en la Web.
 - Protocolos de establecimiento de claves.
 - Protocolo de intercambio de claves Diffie-Hellman.
 - Protocolo basados en servidor Kerberos.
 - Protocolo basados en autenticación robusta mediante X.509.
 - Protocolo TLS/SSL.
- Unidad 12. Correo electrónico seguro.
 - Iniciativa SEEOTI.
 - S/MIME
 - PEM
 - PGP



- Unidad 13. Aplicaciones bancarias y comercio electrónico.

- Introducción. El modelo legal de comercio electrónico: UNCITRAL.
- Protocolo seguro para transacciones con tarjetas de crédito. SET.
- Otros protocolos de pago: iKP, SEPP.
- Monedero y dinero electrónico.

6.EQUIPO DOCENTE

- [ROBERTO HERNANDEZ BERLINCHES](#)
- [IGNACIO JOSE LOPEZ RODRIGUEZ](#)

7.METODOLOGÍA Y ACTIVIDADES DE APRENDIZAJE

La metodología de estudio utiliza la tecnología de formación a distancia en cursos virtuales. En este entorno se trabajarán los contenidos teórico- prácticos cuya herramienta fundamental de comunicación será el curso virtual, utilizando la bibliografía básica y el material complementario. Esta actividad del alumno en el aula virtual corresponde aproximadamente a un 30% del tiempo total asignado al estudio de la asignatura.

El trabajo autónomo de estudio, junto con las actividades de ejercicios y pruebas de autoevaluación disponibles, bajo la supervisión del tutor, con las herramientas y directrices preparadas por el equipo docente, completará aproximadamente un 60% del tiempo de preparación de la asignatura. Por último esta asignatura tiene además programadas unas actividades de evaluación a distancia. Esta actividad formativa representa aproximadamente el 10% del tiempo dedicado a la asignatura.

En la siguiente tabla se muestra su relación con los resultados de aprendizaje y el porcentaje de forma esquemática.

Actividades formativas:	RA relacionados	Número de horas
Preparación estudio contenido teórico	RA4, RA5	30%
Desarrollo de actividades con carácter presencial o en línea (curso virtual)	RA7	10%
Trabajo autónomo	RA7	60%
	TOTAL:	100 %

8.EVALUACIÓN



En esta asignatura se utilizan las modalidades de evaluación continua, pruebas de evaluación a distancia y evaluación final, según se expone a continuación.

- Evaluación continua: Autoevaluación, de carácter voluntario. En esta asignatura se plantea a los alumnos un proceso de autoevaluación, basado en la realización de pruebas de test. Estos ejercicios no serán evaluables. En el módulo de contenidos dentro del entorno virtual de la UNED el alumnado podrán encontrar el apartado de "Autoevaluación" de sus conocimientos.
- Pruebas de evaluación a distancia: En el módulo de contenidos dentro del entorno virtual de la UNED se encontrará el apartado de "Evaluación a distancia" donde se alojarán las pruebas (una por cada Unidad Didáctica) que serán evaluadas por profesorado tutor de los centros, con la ayuda del equipo docente. Consistirán en pequeños trabajos prácticos y alguna cuestión teórica que permitirán comprobar la correcta asimilación de contenidos y la adquisición real de las competencias relacionadas. La calificación de estas actividades corresponden con el 20% de la nota final de la asignatura.
- Evaluación final de la asignatura que se llevará a cabo mediante un examen teórico-práctico, que es necesario aprobar para la superación de la asignatura y que contará como el 80% de la nota final.

Esquemáticamente se puede ver en la siguiente tabla:

Actividades de Evaluación:		% de la nota
Pruebas de evaluación a distancia	Prácticas	20%
Realización de las pruebas presenciales (Examen)		80%

9.BIBLIOGRAFÍA BÁSICA

Comentarios y anexos:

CRIPTOGRAFIA Y SEGURIDAD EN COMPUTADORES
Versión 4-0.9.0
27 de mayo de 2011
MANUEL JOSE LUCENA LOPEZ

10.BIBLIOGRAFÍA COMPLEMENTARIA

LIBRO ACTUALMENTE NO PUBLICADO
ISBN(13):
Título: TÉCNICAS CRIPTOGRÁFICAS DE PROTECCIÓN DE DATOS (3ª)
Autor/es: Fuster, José María ;
Editorial: : RAMA

ISBN(13): 9788436249750
Título: SEGURIDAD EN LAS COMUNICACIONES Y EN LA INFORMACIÓN (1ª)
Autor/es: Castro Gil, Manuel Alonso ; Díaz Orueta, Gabriel ; Peire Arroba, Juan ; Mur Pérez, Francisco ;
Editorial: UNED

Buscarlo en librería virtual UNED

Buscarlo en bibliotecas UNED



Buscarlo en la Biblioteca de Educación

Buscarlo en Catálogo del Patrimonio Bibliográfico

11. RECURSOS DE APOYO

Como materiales adicionales para el estudio de la asignatura se ofrece en el curso virtual:

- Esta guía y la guía didáctica de estudio de la asignatura.
- Distintos libros electrónicos gratuitos, algunos interactivos.
- Material desarrollado exprofeso para el curso por el equipo docente
- Pruebas prácticas de evaluación a distancia.

12. TUTORIZACIÓN

La enseñanza a distancia utilizada para el seguimiento de esta asignatura, que garantiza la ayuda al alumnado disponer de los siguientes recursos:

- Tutores en los centros asociados. Los tutores serán los encargados del seguimiento y control de las pruebas que constituyen la evaluación continua del alumno.
- Tutorías presenciales o virtuales en el centro asociado correspondiente.
- Entorno Virtual. A través del curso virtual el equipo docente de la asignatura pondrá a disposición de los alumnos diverso material de apoyo al estudio, así como el enunciado del trabajo práctico-teórico a distancia.
- Foros de discusión donde los estudiantes podrán plantear sus dudas para que sean respondidas por el profesorado de tutoría o por el propio equipo docente. Este recurso es el SOPORTE FUNDAMENTAL de la asignatura, y supone la principal herramienta de comunicación entre equipo docente y estudiante, así como éstos entre sí.
- Tutorías con el equipo docente: los lunes de 15:00 a 19:00 h para el periodo durante el que se desarrolla la asignatura.

