PROYECTO DOCENTE
ASIGNATURA:
"Criptografía"

Grupo: Clases Teoricas-Prácticas de Criptografia(972131)

Titulacion: Grado en Ingeniería Informática-Tecnologías Informáticas

Curso: 2014 - 2015

DATOS BÁSICOS DE LA ASIGNATURA/GRUPO

Titulación:	Grado en Ingeniería Informática-Tecnologías Informáticas
Año del plan de estudio:	2010
Centro:	E.T.S. Ingeniería Informática
Asignatura:	Criptografía
Código:	2060046
Tipo:	Optativa
Curso:	4º
Período de impartición:	Segundo Cuatrimestre
Ciclo:	0º
Grupo:	Clases Teoricas-Prácticas de Criptografia (1)
Créditos:	6
Horas:	150
Área:	Matemática Aplicada (Área principal)
Departamento:	Matemática Aplicada I (Departamento responsable)
Dirección postal:	
Dirección electrónica:	

COORDINADOR DE LA ASIGNATURA

ARMARIO SAMPALO, JOSE ANDRES

PROFESORADO

1 ARMARIO SAMPALO, JOSE ANDRES
2 VALEIRAS REINA, GERARDO

OBJETIVOS Y COMPETENCIAS

Objetivos docentes específicos

Introducir al alumno en la criptografía, el criptoanálisis y en sus aplicaciones.

Competencias

Competencias transversales/genéricas

Competencias generales

G03 Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas.

G08 Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías,así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

G09 Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

Competencias básicas

E07 Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.

Competencias generales

G03 Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas.

G08 Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías,así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.

G09 Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.

Competencias básicas

E07 Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.

Competencias específicas

Competencias especificas

E48 Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

CONTENIDOS DE LA ASIGNATURA

Relación sucinta de los contenidos (bloques temáticos en su caso)

1. Introducción

Necesidad de la seguridad. No sólo secreto. Ataques y defensas. Ataques pasivos. Ataques activos. Servicios de seguridad. ¿Qué es la Criptografía?. Cifrar y descifrar. Criptoanálisis. Seguridad computacional. Atacantes y sus recursos.

2. Fundamentos

Un poco de historia. Desplazamiento. Cifrado afín. Cifrado por sustitución. Cifrado por transposición. Cifrado de Vigenère. Cifrado XOR. Teoría de la información. Cifrado de Vernam. Cifrados en flujo.

3. Criptografía simétrica

Criptosistemas simétricos. Ventajas e inconvenientes. Cifrado por bloques. Cifrado producto. Cifrados por bloques. DES. AES. IDEA. Otros cifrados simétricos.

4. Criptografía de clave pública

Criptografía de clave pública. El criptosistema de mochila de Merkle-Hellman. El criptosistema RSA. El criptosistema Elgamal. Criptografía de curvas elípticas.

5. Aplicaciones

Sobre digital. Intercambio de claves de Diffie y Hellman. Autenticación e integridad. Funciones resumen. Firmas digitales. Firma digital RSA. Firma digital Elgamal. Certificados digitales. Algunos problemas resueltos.

CONTENIDOS DE LA ASIGNATURA

Relación sucinta de los contenidos (bloques temáticos en su caso)

1. Introducción

Necesidad de la seguridad. No sólo secreto. Ataques y defensas. Ataques pasivos. Ataques activos. Servicios de seguridad. ¿Qué es la Criptografía?. Cifrar y descifrar. Criptoanálisis. Seguridad computacional. Atacantes y sus recursos.

2. Fundamentos

Un poco de historia. Desplazamiento. Cifrado afín. Cifrado por sustitución. Cifrado por transposición. Cifrado de Vigenère. Cifrado XOR. Teoría de la información. Cifrado de Vernam. Cifrados en flujo.

3. Criptografía simétrica

Criptosistemas simétricos. Ventajas e inconvenientes. Cifrado por bloques. Cifrado producto. Cifrados por bloques. DES. AES. IDEA. Otros cifrados simétricos.

4. Criptografía de clave pública

Criptografía de clave pública. El criptosistema de mochila de Merkle-Hellman. El criptosistema RSA. El criptosistema Elgamal. Criptografía de curvas elípticas.

5. Aplicaciones

Sobre digital. Intercambio de claves de Diffie y Hellman. Autenticación e integridad. Funciones resumen. Firmas digitales. Firma digital RSA. Firma digital Elgamal. Certificados digitales. Algunos problemas resueltos.

ACTIVIDADES FORMATIVAS

Relación de actividades formativas del cuatrimestre

Clases teóricas

Horas presenciales: 27.0

Horas no presenciales: 26.0

Metodología de enseñanza-aprendizaje:

Durante 10 semanas, totalizando 27 horas presenciales, se procederá a comentar el contenido teórico de la asignatura, con la ayuda del ordenador, ilustrando la exposición con ejemplos clarificadores. Los alumnos dispondrán de una copia de las presentaciones en ordenador a utilizar en clase, la cual estará accesible tanto en papel (en la copistería del centro), como por conexión de internet (en la página web de la asignatura en el servidor del departamento).

Prácticas de Laboratorio

Horas presenciales: 19.0

Horas no presenciales: 25.0

Metodología de enseñanza-aprendizaje:

Los alumnos tendrán a su disposición en la web de la asignatura un boletín de problemas, algunos de ellos completamente resueltos, eincluyendo exámenes de convocatorias precedentes. Durante 12 semanas, totalizando 19 horas presenciales, en las primeras 10 semanas se procederá a la resolución por parte del profesor, y eventualmente del alumnado, de problemas. En las últimas 2 semanas los alumnos expondrán y defenderán sus trabajos de carácter práctico en el aula.

Prácticas informáticas

Horas presenciales: 8.0

Horas no presenciales: 4.0

Competencias que desarrolla:

Las clases de laboratorio comenzarán a partir de la undécima semana hasta la semana duodécima, totalizando 8 horas presenciales. En estas clases, el profesor se dedicará fundamentalmente a resolver dudas técnicas y científicas, asesorar, y a ayudar a diseñar las diferentes aplicaciones informáticas correspondientes a los trabajos prácticos dirigidos asignados.

AAD sin presencia del profesor

Horas presenciales: 0.0

Horas no presenciales: 21.0

Metodología de enseñanza-aprendizaje:

Los alumnos se organizaran en grupos. A cada grupo se le asignará un trabajo de un listado difundido en la web durante las primerassemanas del curso. Este trabajo se desarrollará a partir de un artículo internacional o algún tema de fácil documentación y actualidad en el área de la Criptografía. Este trabajo consistirá en la asimilación de estos documentos y elaboración de una memoria y, si fuera posible, el desarrollo de un programa informático. Las últimas semanas de clase se dedicarán a la exposición y defensa de estos trabajos por parte de todos los grupos (deberán exponer todos los integrantes del grupo). El profesor dedicará unos 60 minutos a supervisar el trabajo realizado por los grupos, previamente a la exposición

Exámenes

Horas presenciales: 6.0

Horas no presenciales: 0.0

Clases teóricas

Horas presenciales: 0.0

Horas no presenciales: 0.0

Horas de estudio

Horas presenciales: 0.0

Horas no presenciales: 14.0

BIBLIOGRAFÍA E INFORMACIÓN ADICIONAL

Bibliografía general

A Friendly introduction to Number Theory

Autores: Silverman, J.H. ***Edición:*** 1997

Publicación: ***ISBN:*** 0-13-263799-5

Number Theory with Computer Applications

Autores: Kumanduri, R., Romero, C. ***Edición:*** 1998

Publicación: ***ISBN:*** 0-13-801812-X

Bibliografía específica

Cryptography :A Primer

Autores: Konheim, A. G. ***Edición:*** 1981

Publicación: ***ISBN:*** 0-471-08132-9

Applied Cryptography Second Edition :Protocols, Algorithms and Source Code in C

Autores: Schneier, B. ***Edición:*** 1996

Publicación: ***ISBN:*** 0-471-11709-9

Network Security :Private Communications in a Public World

Autores:	Kaufman, C., Perlman, R., Speciner, M.	***Edición:***	1995
Publicación:		***ISBN:***	0-13-061466-1

Cryptography :theory and practice

Autores:	Stinson, D.R.	***Edición:***	1995
Publicación:		***ISBN:***	0-8493-8521-0

Cryptography and Network Security :Principles and Practice

Autores:	Stallings, W.	***Edición:***	1999
Publicación:		***ISBN:***	0-13-869017-0

Handbook of Applied Cryptography

Autores:	Menezes, A. J., Van Oorschot, P. C. and Vanstone, S. A	***Edición:***	1996
Publicación:		***ISBN:***	

Criptografía y seguridad en computadore

Autores:	Lucena López, M.J.	***Edición:***	
Publicación:		***ISBN:***	

Sistema de evaluación

Evaluación continua

El sistema de evaluación por curso comprende tres apartados distintos: exposición de un trabajo en grupo (sobre 4.5 puntos), seguimiento de las exposiciones de los trabajos (sobre 1 punto) y examen teórico-práctico (sobre 4.5 puntos).
La calificación final resulta de la suma de las tres calificaciones parciales anteriores. Se considera que un alumno supera la asignatura cuando su calificación final es 5 o superior, siempre y cuando haya obtenido un mínimo de un punto en el examen teórico-práctico, así como un punto en la exposición del trabajo en grupo.

Examen final

Aquellos alumnos que no hayan superado la asignatura por el sistema de evaluación por curso, o que por decisión personal renuncien a la nota de evaluación por curso, tienen la opción de superar la asignatura por medio de un examen teórico-práctico final (evaluado sobre 10 puntos), a celebrar en cada una de las convocatorias oficiales de la asignatura. Se considera que un alumno supera la asignatura cuando su calificación final es 5 o superior.

CALENDARIO DE EXÁMENES

La información que aparece a continuación es susceptible de cambios por lo que le recomendamos que la confirme con el Centro cuando se aproxime la fecha de los exámenes.

1 ª Convocatoria

CENTRO: E.T.S. Ingeniería Informática

Fecha:	15/6/2015	***Hora:***	Por definir
Aula:	Por definir		

2 ª Convocatoria

CENTRO: E.T.S. Ingeniería Informática

Fecha:	2/9/2015	***Hora:***	Por definir
Aula:	Por definir		

Diciembre

CENTRO: E.T.S. Ingeniería Informática

Fecha:	3/12/2014	***Hora:***	Por definir
Aula:	Por definir		

TRIBUNALES ESPECÍFICOS DE EVALUACIÓN Y APELACIÓN

Presidente:	ELENA MARTIN GARCIA
Vocal:	VICTOR ALVAREZ SOLANO
Secretario:	MARIA DOLORES FRAU GARCIA
Primer suplente:	ALBERTO MARQUEZ PEREZ
Segundo suplente:	AMPARO OSUNA LUCENA
Tercer suplente:	ANTONIO JESUS CAÑETE MARTIN

ANEXO 1:

HORARIOS DEL GRUPO DEL PROYECTO DOCENTE

Los horarios de las actividades no principales se facilitarán durante el curso.

GRUPO: Clases Teoricas-Prácticas de Criptografia (972131)

Calendario del grupo

CLASES DEL PROFESOR: ARMARIO SAMPALO, JOSE ANDRES

HORARIO SIN ESPECIFICAR