Proyecto/Guía Docente de la asignatura

Asignatura	Protocolos y Comunicaciones Seguras		
Materia	Matemáticas		
Módulo			
Titulación	Grado en Ingeniería Informática de Servicios y Aplicaciones		
Plan	413 / 5471 / 5472	**Código**	40843
Periodo de impartición	Semestre 7	**Tipo/Carácter**	OP
Nivel/Ciclo	Grado	**Curso**	4
Créditos ECTS	6		
Lengua en que se imparte	Español		
Profesor responsable	José Ignacio Farrán Martín		
Datos de contacto (E-mail, teléfono…)	Escuela de Ingeniería Informática Plaza de la Universidad 1 - 40005 Segovia Teléfono : (+34) 921 11 24 20 Fax : (+34) 921 11 24 01 e-mail : jifarran@eii.uva.es web : http://wmatem.eis.uva.es/~ignfar		
Horario de tutorías	Ver http://campusvirtual.uva.es		
Departamento	Matemática Aplicada		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

Esta asignatura estudia las técnicas matemáticas relacionadas con el cifrado de datos, el criptoanálisis y sus aplicaciones en la Seguridad Informática. Se introducirán los principios básicos de la criptografía de clave privada y de clave pública, así como los protocolos criptográficos de utilidad en diversas aplicaciones prácticas.

1.2 Relación con otras materias

Esta asignatura será referencia teórica de otras más prácticas como “Seguridad Informática” o “Comercio Electrónico”. Se recomienda tener superadas las asignaturas de primer curso, en especial “Matemática Discreta”, “Álgebra Lineal y Geometría”, “Cálculo de Probabilidades y Estadística” y “Estructura y Tecnología de Computadores”, así como las asignaturas de “Tratamiento Automático de la Información”, “Redes de Computadores” y “Seguridad Informática”.

1.3 Prerrequisitos

Ninguno.

2. Competencias

2.1 Generales

G01 : Conocimientos generales básicos.
G03 : Capacidad de análisis y síntesis.
G05 : Comunicación oral y escrita en la lengua propia.
G06 : Conocimiento de una segunda lengua (Inglés).
G07 : Habilidades básicas en el manejo del ordenador.
G09 : Resolución de problemas.
G16 : Capacidad de aplicar los conocimientos en la práctica.
G18 : Capacidad de aprender.

2.2 Específicas

E01 : Capacidad para la resolución de los problemas matemáticos que puedan plantearse en la ingeniería. Aptitud para aplicar los conocimientos sobre: álgebra lineal; cálculo diferencial e integral; métodos numéricos; algorítmica numérica; estadística y optimización.
E02 : Comprensión y dominio de los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para el tratamiento automático de la información por medio de sistemas computacionales y para la resolución de problemas propios de la ingeniería.
E03 : Conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería.
E11 : 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.

3. Objetivos

- Plantear en lenguaje matemático y resolver problemas relacionados con la representación matemática de la información, su encriptación, y sus aplicaciones en la Seguridad Informática.
- Describir algorítmicamente la resolución de problemas relativos a la encriptación de datos, e implementarla eficientemente mediante software matemático.
- Comprender, discutir y expresar (oralmente y por escrito) conceptos y argumentos de tipo lógico matemático relacionados con la Seguridad Informática.
- Construcción de los modelos matemáticos necesarios para la resolución de problemas aplicados a la Seguridad Informática y su uso en la Empresa.
- Manejar software matemático en aplicaciones prácticas, con un énfasis especial en la interpretación de resultados y la escritura de informes.
- Comprender la interrelación de la Criptología con otras materias de la titulación.

4. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas (T/M)	28	Estudio y trabajo autónomo individual	50
Clases prácticas de aula (A)		Estudio y trabajo autónomo grupal	40
Laboratorios (L)	28		
Prácticas externas, clínicas o de campo			
Seminarios (S)			
Tutorías grupales (TG)			
Evaluación	4		
Total presencial	**60**	**Total no presencial**	**90**

5. Métodos docentes y principios metodológicos

A lo largo de la asignatura se realizará una actividad de **aprendizaje basado en proyectos**, que permitirá llevar a la práctica los conocimientos adquiridos a nivel teórico. La organización de esta actividad responderá a los principios y valores establecidos en el Proyecto de Innovación Docente **UVagile**, de tal forma que el alcance del proyecto se dividirá en *sprints de aprendizaje* de una duración similar. El proyecto se realizará en equipos de trabajo de entre 3 y 5 alumnos, y tendrá entregas parciales a lo largo del cuatrimestre con el objetivo de retroalimentar su desarrollo. Finalmente, cabe destacar que los equipos de trabajo dispondrán de diferentes herramientas digitales para facilitar la organización y coordinación de sus tareas, además de para la comunicación tanto entre los miembros de cada equipo como con el propio profesor de la asignatura.

6. Bloques temáticos

Bloque 1:Criptología y comunicaciones seguras

Carga de trabajo en créditos ECTS: 1,6

a. Contextualización y justificación

Este tema sirve de introducción a los fundamentos matemáticos de la criptología. Por un lado se introducen los conceptos básicos de cifrado, clave y seguridad matemática, así como los sistemas clásicos de cifrado que se han sucedido en la historia. Por otro, se estudian los métodos básicos de esteganografía y criptoanálisis.

b. Objetivos de aprendizaje

- Conocer los conceptos básicos de la seguridad informática y la criptología.
- Análisis con perspectiva histórica de los métodos clásicos de cifrado y esteganográficos.
- Estudiar de manera teórico-práctica los métodos básicos de criptoanálisis.

c. Contenidos

1. Conceptos básicos: seguridad y criptosistemas.
2. Criptología y esteganografía.
3. Métodos clásicos de cifrado de datos.
4. Introducción al criptoanálisis.

d. Métodos docentes

1. Lección magistral: exposición de la teoría (8 horas).
2. Prácticas: resolución de problemas, prácticas de ordenador, y realización de Proyecto (8 horas).
3. Estudio autónomo por parte del alumno, incluyendo realización de problemas, consulta bibliográfica, realización de prácticas y preparación de pruebas de evaluación (mínimo 24 horas).

e. Plan de trabajo

Alternar sesiones teóricas con clases de problemas y prácticas de ordenador.

f. Evaluación

Método de proyectos: evaluación global al final del curso.

g. Bibliografía básica

A. Fúster et al.: *Técnicas criptográficas de protección de datos (3ª edición)*, Ed. Ra-Ma (2004).
M. Lutz: *Python Pocket Reference*, O'Reilly (2014).

h. Bibliografía complementaria

B. Schneier: *Applied Cryptography*, John Wiley & Sons (1996).
G. J. Simmons: *Contemporary Cryptology*, IEEE Press (1992).
M. Lutz: *Learning Python*, O'Reilly (2014).

i. Recursos necesarios

Aula con pizarra y ordenador con proyector, laboratorio de informática con software matemático, biblioteca, sala de estudio, y despacho o seminario para tutorías.

Bloque 2:Criptografía simétrica

Carga de trabajo en créditos ECTS: 1,6

a. Contextualización y justificación

Este tema introduce los diferentes tipos de cifrado simétrico, tanto en flujo como en bloque, junto con la gestión de claves y las aplicaciones y protocolos de clave simétrica.

b. Objetivos de aprendizaje

- Conocer las técnicas básicas de cifrado simétrico.
- Conocer las técnicas básicas de gestión de claves.
- Conocer los protocolos básicos de clave simétrica.

c. Contenidos

1. Cifrado en flujo.
2. Cifrado en bloque.
3. Gestión de claves.
4. Aplicaciones.

d. Métodos docentes

1. Lección magistral: exposición de la teoría (8 horas).
2. Prácticas en aula: realización de Proyecto (8 horas).
3. Estudio autónomo por parte del alumno, incluyendo realización de problemas, consulta bibliográfica, realización de prácticas y preparación de pruebas de evaluación (mínimo 24 horas).

e. Plan de trabajo

Alternar sesiones teóricas con clases de problemas y prácticas de ordenador.

f. Evaluación

Método de proyectos: evaluación global al final del curso.

g. Bibliografía básica

A. Fúster et al.: *Técnicas criptográficas de protección de datos (3ª edición)*, Ed. Ra-Ma (2004).
M. Lutz: *Python Pocket Reference*, O'Reilly (2014).

h. Bibliografía complementaria

B. Schneier: *Applied Cryptography*, John Wiley & Sons (1996).
G. J. Simmons: *Contemporary Cryptology*, IEEE Press (1992).
M. Lutz: *Learning Python*, O'Reilly (2014).

i. Recursos necesarios

Aula con pizarra y ordenador con proyector, laboratorio de informática con software matemático, biblioteca, sala de estudio, y despacho o seminario para tutorías.

Bloque 3:Algoritmos básicos

Carga de trabajo en créditos ECTS: 0,8

a. Contextualización y justificación

Este tema, de carácter técnico, proporciona los fundamentos teóricos de la seguridad basada en problemas computacionalmente complejos, y repasa en primer lugar los algoritmos esenciales de la teoría de números enteros. Asimismo, se introducen las llamadas funciones unidireccionales y las funciones Hash, que son la base práctica de los sistemas criptográficos de clave pública.

b. Objetivos de aprendizaje

- Conocer los conceptos matemáticos subyacentes en la llamada seguridad computacional.
- Repasar los algoritmos fundamentales de la aritmética entera y modular.
- Conocer ejemplos de las llamadas funciones unidireccionales y sus propiedades esenciales.
- Conocer los fundamentos básicos de las llamadas funciones Hash.

c. Contenidos

1. Complejidad Computacional.
2. Algoritmos fundamentales de la Teoría de Números.
3. Funciones unidireccionales (One-Way).
4. Funciones resumen (Hash).

d. Métodos docentes

1. Lección magistral: exposición de la teoría (4 horas).
2. Prácticas en aula: realización de Proyecto (4 horas).
3. Estudio autónomo por parte del alumno, incluyendo realización de problemas, consulta bibliográfica, realización de prácticas y preparación de pruebas de evaluación (mínimo 12 horas).

e. Plan de trabajo

Alternar sesiones teóricas con clases de problemas y prácticas de ordenador.

f. Evaluación

Método de proyectos: evaluación global al final del curso.

g. Bibliografía básica

A. Fúster et al.: *Técnicas criptográficas de protección de datos (3ª edición)*, Ed. Ra-Ma (2004).
M. Lutz: *Python Pocket Reference*, O'Reilly (2014).

h. Bibliografía complementaria

B. Schneier: *Applied Cryptography*, John Wiley & Sons (1996).
G. J. Simmons: *Contemporary Cryptology*, IEEE Press (1992).
M. Lutz: *Learning Python*, O'Reilly (2014).

i. Recursos necesarios

Aula con pizarra y ordenador con proyector, laboratorio de informática con software matemático, biblioteca, sala de estudio, y despacho o seminario para tutorías.

Bloque 4:Criptografía de clave pública

Carga de trabajo en créditos ECTS: 1,2

a. Contextualización y justificación

Este tema proporciona las técnicas matemáticas básicas de la llamada criptografía de clave pública, y sus aplicaciones a través de la firma digital. En particular, se estudian los criptosistemas RSA y de ElGamal, así como el sistema de intercambio de claves de Diffie-Hellman.

b. Objetivos de aprendizaje

- Conocer el sistema de intercambio de claves de Diffie-Hellman.
- Conocer los sistemas criptográficos RSA y de ElGamal.
- Conocer el concepto de firma digital y sus aplicaciones.

c. Contenidos

1. Intercambio de claves de Diffie-Hellman.
2. Criptosistema RSA.
3. Criptosistema de ElGamal.
4. Firma digital y aplicaciones.

d. Métodos docentes

1. Lección magistral: exposición de la teoría (6 horas).
2. Prácticas en aula: práctica individual y realización de Proyecto (6 horas).
3. Estudio autónomo por parte del alumno, incluyendo realización de problemas, consulta bibliográfica, realización de prácticas y preparación de pruebas de evaluación (mínimo 18 horas).

e. Plan de trabajo

Alternar sesiones teóricas con clases de problemas y prácticas de ordenador.

f. Evaluación

Entrega de una práctica individual de ordenador.
Método de proyectos: evaluación global al final del curso.

g. Bibliografía básica

A. Fúster et al.: *Técnicas criptográficas de protección de datos (3ª edición)*, Ed. Ra-Ma (2004).
M. Lutz: *Python Pocket Reference*, O'Reilly (2014).

h. Bibliografía complementaria

B. Schneier: *Applied Cryptography*, John Wiley & Sons (1996).
G. J. Simmons: *Contemporary Cryptology*, IEEE Press (1992).
M. Lutz: *Learning Python*, O'Reilly (2014).

i. Recursos necesarios

Aula con pizarra y ordenador con proyector, laboratorio de informática con software matemático, biblioteca, sala de estudio, y despacho o seminario para tutorías.

Bloque 5:Protocolos criptográficos

Carga de trabajo en créditos ECTS: 0,8

a. Contextualización y justificación

Este tema final muestra la verdadera potencia de la criptografía de clave pública y la firma digital, a través de diversos protocolos criptográficos que pueden aplicarse en multitud de situaciones prácticas.

b. Objetivos de aprendizaje

- Comprender la potencia y aplicaciones de los protocolos de clave pública.
- Identificar situaciones prácticas en donde se pueden aplicar dichos protocolos criptográficos.

c. Contenidos

1. Autenticación de mensajes.
2. Identificación de usuarios.
3. Compartición de secretos.
4. Venta de secretos.
5. Intercambio de secretos.
6. Esquema electoral.
7. Firma de contratos.
8. Correo con acuse de recibo.

d. Métodos docentes

1. Lección magistral: exposición de la teoría (2 horas).
2. Prácticas en aula: realización de Proyecto (2 horas).
3. Evaluación (4 horas).
4. Estudio autónomo por parte del alumno, incluyendo realización de problemas, consulta bibliográfica, realización de prácticas y preparación de pruebas de evaluación (mínimo 12 horas).

e. Plan de trabajo

Alternar sesiones teóricas y prácticas de ordenador con seminarios para la exposición y evaluación del Proyecto final.

f. Evaluación

Entrega y defensa del Proyecto en grupo, y trabajo teórico opcional.

g. Bibliografía básica

A. Fúster et al.: *Técnicas criptográficas de protección de datos (3ª edición)*, Ed. Ra-Ma (2004).
M. Lutz: *Python Pocket Reference*, O'Reilly (2014).

h. Bibliografía complementaria

B. Schneier: *Applied Cryptography*, John Wiley & Sons (1996).
G. J. Simmons: *Contemporary Cryptology*, IEEE Press (1992).
M. Lutz: *Learning Python*, O'Reilly (2014).

i. Recursos necesarios

Aula con pizarra y ordenador con proyector, laboratorio de informática con software matemático, biblioteca, sala de estudio, y despacho o seminario para tutorías.

7. Temporalización (por bloques temáticos)

BLOQUE TEMÁTICO	CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
1. Criptología y comunicaciones seguras	1,6	4 semanas
2. Criptografía simétrica	1,6	4 semanas
3. Algoritmos básicos	0,8	2 semanas
4. Criptografía de clave pública	1,2	3 semanas
5. Protocolos criptográficos	0,8	2 semanas

8. Tabla resumen de los instrumentos, procedimientos y sistemas de evaluación/calificación

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Resolución en grupo de problemas prácticos con ordenador.	25%	Al finalizar el bloque temático 1.
Realización de un Proyecto de software en grupo sobre los contenidos del curso.	75%	Se entregará una Memoria, y se expondrá en clase el Proyecto con una demo, durante la última semana del curso.

CRITERIOS DE CALIFICACIÓN

• **Convocatoria ordinaria:**
  ○ De no superar la asignatura mediante la evaluación continua anteriormente descrita, se realizará un examen teórico-práctico que aportará el 100% de la nota.
• **Convocatoria extraordinaria:**
  ○ Los mismos que en la convocatoria ordinaria.

9. Consideraciones finales

Es REQUISITO IMPRESCINDIBLE para poder acogerse a la evaluación continua la asistencia a clase en al menos el 50% de las clases. En caso contrario, se disponen de las dos convocatorias oficiales de examen, ordinaria y extraordinaria. Por tanto, la asistencia a clase no es requisito para aprobar, ni se valora en la nota, es simplemente un requisito necesario para poder realizar la evaluación continua.

Aun habiendo aprobado en la evaluación continua, cualquier alumno puede presentarse voluntariamente con toda la materia al examen ordinario para subir nota, y esta sería entonces la máxima de las dos notas obtenidas.

No se guardará ninguna nota de la evaluación continua para las convocatorias ordinaria y extraordinaria en caso de suspenso en la evaluación continua.