Asignatura: Fundamentos de Criptografía y Seguridad Informática
Código: 18765
Centro: Escuela Politécnica Superior
Titulación: Grado en Ingeniería Informática
Nivel: Grado
Tipo: Optativa
Nº de créditos: 6

GUÍA DOCENTE DE FUNDAMENTOS DE CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

La presente guía docente corresponde a la asignatura Fundamentos de Criptografía y Seguridad Informática (F-CSI), aprobada para el curso lectivo 2017-2018 en Junta de Centro y publicada en su versión definitiva en la página web de la Escuela Politécnica Superior. La guía docente de F-CSI aprobada y publicada antes del periodo de matrícula tiene el carácter de contrato con el estudiante.

ASIGNATURA

FUNDAMENTOS DE CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA (F-CSI)

1.1. Código

18765 del Grado en Ingeniería Informática

1.2. Materia

Materias de Sistemas de Información y Tecnologías de Información

1.3. Tipo

Optativa

1.4. Nivel

Grado

1.5. Curso

4º

1.6. Semestre

1º

1.7. Número de créditos

6 créditos ECTS

1.8. Requisitos previos

Fundamentos de Criptografía y Seguridad Informática forma parte de la optatividad de las materias de Sistemas de Información y Tecnologías de Información del último año del plan de estudios del Grado en Ingeniería Informática, que proporcionan formación en aspectos avanzados de la Ingeniería Informática. Esta asignatura se imparte en el primer semestre del cuarto curso. Siendo una asignatura de fundamentos, no se establecen requisitos específicos previos a ese respecto. Sin embargo, dado que se van a estudiar los principales algoritmos criptográficos y su uso en seguridad informática se requiere cierta madurez en el uso y comprensión de

algoritmos. La asignatura incluye una parte importante dedicada a la implementación de estos algoritmos, para la cual el alumno precisa disponer de un buen nivel de programación en C, resultante de las asignaturas de los cursos anteriores.

Se recomienda para garantizar la asimilación de los contenidos y la adquisición de habilidades la lectura crítica de los textos de la bibliografía, el uso del material electrónico de esta asignatura disponible en la plataforma Moodle (http://uam-virtual.es) y la búsqueda activa de material complementario en la red. Es recomendable disponer de un dominio de inglés que permita al alumno leer la bibliografía de consulta.
La asignatura está dirigida a enseñar los fundamentos de la Criptografía clásica y moderna y sus implicaciones en Seguridad Informática. Se pretende dar al alumno una base profunda de la fortaleza y la debilidad de los diversos métodos de cifrado y su aplicación a seguridad informática. Por ello, los algoritmos de cifrado se acompañan de los métodos para criptoanalizarlos, con el objetivo de analizar su robustez. Ello se complementa con el trabajo aplicado en los laboratorios para el desarrollo de las habilidades prácticas, y la comprensión de su conexión con los fundamentos teóricos. Se requiere asimismo iniciativa personal y constancia para desarrollar estas actividades durante el curso. Finalmente, se requiere predisposición y empatía para el trabajo colaborativo en grupo.

1.9. Requisitos mínimos de asistencia a las sesiones presenciales

Se plantean dos itinerarios, uno con asistencia obligatoria a clase y otro sin ella, los estudiantes deberán optar por uno u otro desde el principio del curso y cumplir con los distintos requisitos de evaluación que conlleva cada uno de los modelos, publicados en la presente guía docente (ver apartado 4).

ITINERARIO CON ASISTENCIA OBLIGATORIA A CLASE
La asistencia es obligatoria al menos en un 85%.

ITINERARIO SIN ASISTENCIA OBLIGATORIA A CLASE
La asistencia es muy recomendable aunque no obligatoria.

1.10. Datos del equipo docente

Nota: se debe añadir @uam.es a todas las direcciones de correo electrónico.

Profesor de teoría:

Dr. Francisco de Borja Rodríguez Ortiz (Coordinador)
Departamento de Ingeniería Informática
Escuela Politécnica Superior
Despacho - Módulo: B-328 Edificio B – 3ª Planta
Teléfono: +34 91 497 2236
Correo electrónico: f.rodriguez
Página web: http://www.eps.uam.es/~frodrig
Horario de atención al alumnado: Petición de cita previa por correo electrónico.

Profesores de prácticas:

Dr. Francisco de Borja Rodríguez Ortiz (Coordinador)
Departamento de Ingeniería Informática
Escuela Politécnica Superior
Despacho - Módulo: B-328 Edificio B – 3ª Planta
Teléfono: +34 91 497 2236
Correo electrónico: f.rodriguez
Página web: http://www.eps.uam.es/~frodrig
Horario de atención al alumnado: Petición de cita previa por correo electrónico.

1.11. Objetivos del curso

F-CSI pretende dar al alumno una base profunda de la fortaleza y la debilidad de los diversos métodos de cifrado y su aplicación a seguridad informática. No es el objeto de esta asignatura que se sepan muchos métodos de cifrado modernos, sino que se conozcan los métodos básicos lo suficientemente bien como para poder construir sus propios cifrados utilizando los principios de diseño aprendidos. El objetivo final del curso no consiste en que hayan memorizado los métodos más punteros de cifrado, Mac y Hash, sino que cuando se les presente algún algoritmo de cifrado o protocolo de seguridad sepan determinar con la ayuda de los conceptos aprendidos cómo es de seguro, cuál es su eficiencia, y en qué circunstancias puede ser utilizado para la seguridad Informática.

Las **competencias** que se persiguen adquirir con esta asignatura son:
Competencias Generales y transversales
1. Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.
Competencias de formación básica
B3. Capacidad para comprender y dominar los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para la resolución de problemas propios de la ingeniería.
Comunes a la rama de informática
C1. 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.
C6. 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.
C8. Capacidad para analizar, diseñar, construir y mantener aplicaciones de forma robusta, segura y eficiente, eligiendo el paradigma y los lenguajes de programación más adecuados.
De tecnología específica:
A) Ingeniería del software
IS5. Capacidad de identificar, evaluar y gestionar los riesgos potenciales asociados que pudieran presentarse.
B) Ingeniería de computadores
IC6. Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
C) Computación
CC3. Capacidad para evaluar la complejidad computacional de un problema, conocer estrategias algorítmicas que puedan conducir a su resolución y recomendar, desarrollar e implementar aquella que garantice el mejor rendimiento de acuerdo con los requisitos establecidos.
D) Sistemas de Información

SI2. Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente.
SI5. Capacidad para comprender y aplicar los principios de la evaluación de riesgos y aplicarlos correctamente en la elaboración y ejecución de planes de actuación.
E) Tecnologías de la Información
TI6. Capacidad de concebir sistemas, aplicaciones y servicios basados en tecnologías de red, incluyendo Internet, web, comercio electrónico, multimedia, servicios interactivos y computación móvil.
TI7. Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

Los objetivos a los que se enfoca esta asignatura son:

OBJETIVOS GENERALES	
G1	Conocer los fundamentos de la criptografía clásica y moderna y sus implicaciones directas en seguridad Informática
G2	Conocer los protocolos básicos orientados a la confidencialidad, autenticación y firma digital en seguridad informática, y además y como se implementan estos mediante las primitivas criptográficas
G3	Conocer la eficiencia y en qué circunstancias pueden ser utilizados los diversos algoritmos de cifrado y protocolos de seguridad para conseguir la seguridad de los sistemas informáticos.

OBJETIVOS ESPECIFICOS POR TEMA	
UNIDAD 1.- Introducción criptografía y seguridad informática	
1.1.	Introducir los conceptos básicos de criptografía y seguridad informática
1.2.	Introducir los servicios de seguridad informática que proporciona la criptografía
1.3.	Hacer una revisión histórica de los principales hitos de criptografía
1.4.	Definir y conocer básicamente algunos modelos y estándares de seguridad informática
UNIDAD 2.- Métodos clásicos de cifrado y criptoanálisis	
2.1.	Conocer y formalizar lo métodos clásicos de cifrado para entender los modelos de seguridad informática actuales
2.2.	Formalizar y resolver problemas sencillos problemas de teoría de números aplicados a criptografía y seguridad informática
2.3.	Establecer la relación de estos métodos clásicos de cifrado con los que se utilizan hoy en día.
2.4.	Estudiar de manera práctica el concepto de criptoanálisis con los métodos de cifrado estudiados
UNIDAD 3.- Criptografía teórica: cifrado perfecto y distancia de unicidad	
3.1.	Introducir un marco teórico para el estudio y análisis de las funciones primitivas criptográficas
3.2.	Establecer los fundamentos del criptoanálisis a través de este marco teórico
3.3.	Aplicar este marco teórico para deducir el concepto de cifrado perfecto y distancia de unicidad de un criptosistema

3.4.	Entender cuales son la implicaciones de cifrado perfecto y distancia de unicidad en la criptografía moderna hoy en día y su aplicación a la seguridad de los sistemas de información
UNIDAD 4.- Criptografía Simétrica	
4.1.	Establecer los fundamentos de seguridad de la criptografía simétrica y su aplicación a seguridad informática
4.2.	Estudiar los principales algoritmos de criptografía simétrica, desde el foco de complejidad algorítmica hasta su aplicación en seguridad informática
4.3.	Estudio de las principales vulnerabilidades y ataques que se dan en criptografía simétrica
UNIDAD 5.- Criptografía pública	
5.1.	Establecer los fundamentos de seguridad de la criptografía pública y su aplicación a seguridad informática
5.2.	Estudiar los principales algoritmos de criptografía pública, desde el foco de complejidad algorítmica hasta su aplicación en seguridad informática
5.3.	Estudio de las principales vulnerabilidades y ataques que se dan en criptografía pública
UNIDAD 6.- Seguridad informática de protocolos: Mac y Hash	
6.1.	Entender los aspectos básicos y protocolos de seguridad en redes de comunicación
6.2.	Identificar las principales vulnerabilidades y amenazas en un sistema de información desde el punto de vista criptográfico
6.3.	Aplicar la funciones primitivas criptográficas a la seguridad informática de protocolos
6.4.	Estudiar la funciones Mac y Hash para su uso en seguridad informática
6.5.	Estudio de las principales vulnerabilidades y ataques que se dan en las funciones Hash

1.12. Contenidos del programa

Programa Sintético

UNIDAD 1. Introducción criptografía y seguridad informática
UNIDAD 2. Métodos clásicos de cifrado y criptoanálisis
UNIDAD 3. Criptografía teórica: cifrado perfecto y distancia de unicidad
UNIDAD 4. Criptografía Simétrica
UNIDAD 5. Criptografía Pública
UNIDAD 6. Seguridad informática de protocolos: Mac y Hash

Programa Detallado

1. **Introducción criptografía y seguridad informática**
   1.1. Definiciones básicas
   1.2. Contexto histórico de la criptografía
   1.3. Esquema general de cifrado y servicios proporcionados a la seguridad informática
   1.4. Tipos de ataques

1.5. Modelos y estándares de seguridad informática, auditoría y certificación

2. **Métodos clásicos de cifrado y criptoanálisis**
   2.1. Definición de criptosistema
   2.2. Criptografía
      2.2.1. Cifrado por desplazamiento
      2.2.2. Cifrado por sustitución
      2.2.3. Cifrado afín
      2.2.4. Cifrado Vigenere
      2.2.5. Cifrado de Hill
      2.2.6. Cifrado por permutación
      2.2.7. Introducción a cifrados de flujo
   2.3. Criptoanálisis y ataques de seguridad
      2.3.1. Principios de Kerchhoff
      2.3.2. Repaso de tipos de ataque
      2.3.3. Ataque genérico sobre métodos monoalfabéticos
      2.3.4. Ataque sobre el método de sustitución
      2.3.5. Ataque genérico sobre métodos polialfabéticos
         2.3.5.1. Test de Kasiski
         2.3.5.2. Índices de coincidencia
      2.3.6. Ataque de texto conocido sobre el método de Hill

3. **Criptografía teórica: cifrado perfecto y distancia de unicidad**
   3.1. Marco teórico para la criptografía y seguridad informática
   3.2. Secreto perfecto
      3.2.1. Seguridad computacional
      3.2.2. Seguridad incondicional
   3.3. Seguridad perfecta en un criptosistema
      3.3.1. Definición y argumentación
      3.3.2. Ejemplos: cifrado por desplazamiento
      3.3.3. Teorema del cifrado perfecto
      3.3.4. El cifrado de Vernam
   3.4. Entropía de los textos planos y cifrados
   3.5. Redundancia del lenguaje
   3.6. Distancia de unicidad y claves espurias

4. **Criptografía Simétrica**
   4.1. Fundamentos genéricos de los cifrados simétricos
      4.1.1. Confusión y difusión
      4.1.2. Producto de criptosistemas: sustitución y permutación
      4.1.3. Cifrado de Feistel: Base del DES, FEAL y otros
   4.2. El Data Encryption Standard (DES)
      4.2.1. Historia
      4.2.2. Descripción del algoritmo
      4.2.3. Principios del diseño
      4.2.4. Propiedades
      4.2.5. Modos de operación
      4.2.6. Tipos de Ataque y vulnerabilidades

- 4.2.7. El DES doble y DES triple
- 4.3. El Advanced Encryption Standard (AES)
  - 4.3.1. Historia
  - 4.3.2. Conceptos previos sobre Rijndael
  - 4.3.3. Operaciones básicas del AES
  - 4.3.4. Criterios y fundamentos de diseño para el AES
  - 4.3.5. Descripción del algoritmo
  - 4.3.6. Algoritmo equivalente para el descifrado
  - 4.3.7. Implementación en micros de 8 bits ("smart cards") y 32 bits (PCs)
  - 4.3.8. Modos de operación

5. Criptografía pública

- 5.1. Esquema genérico de cifrado público
- 5.2. Fundamentos genéricos de los cifrados asimétricos
  - 5.2.1. Funciones de una sola dirección
  - 5.2.2. Funciones Trapdoor
  - 5.2.3. Ejemplos con aritmética modular
- 5.3. El algoritmo del RSA
  - 5.3.1. Fundamentos matemáticos
  - 5.3.2. Generación de claves
  - 5.3.3. Función de cifrado RSA
  - 5.3.4. Algoritmo de potenciación modular óptima
  - 5.3.5. Generación de números primos grandes
  - 5.3.6. Algoritmo de Miller-Rabin
  - 5.3.7. Primos fuertes
  - 5.3.8. Inyectividad del RSA
  - 5.3.9. Tipos de ataques y vulnerabilidades sobre el RSA

6. Seguridad informática de protocolos: Mac y Hash

- 6.1. Servicios suministrados para seguridad informática a través de las primitivas criptográficas.
  - 6.1.1. Confidencialidad
  - 6.1.2. Integridad
  - 6.1.3. Autenticación de mensajes
  - 6.1.4. Firma digital
- 6.2. Vulnerabilidades de los servicios suministrados
- 6.3. Justificación de las funciones FCS: Mac y Hash
- 6.4. Funciones MAC
  - 6.4.1. Propiedades
  - 6.4.2. Ejemplos de construcción de funciones MAC
  - 6.4.3. Ejemplos de protocolos MAC
- 6.5. Funciones Hash
  - 6.5.1. Propiedades
  - 6.5.2. Estructura de funciones Hash
  - 6.5.3. Ejemplos de protocolos Hash
  - 6.5.4. Debilidades y vulnerabilidades de las funciones Hash

1.13. Referencias de consulta

Bibliografía:

Nota: Esta asignatura no sigue ningún libro en concreto. La lectura recomendada se indica por orden de afinidad al contenido del programa:

1. D. R. Stinson, "Cryptography: Theory and Practice" (Básica).
2. W. Stallings, "Cryptography and Network Security: Principles and Practice" (Básica).
3. A. J. Menezes, P. C.van Oorschot, S. A. Vanstone, "Handbook of Applied Cryptography" (Complementaria).
4. B. Schneier, "Applied Cryptography" (Complementaria).
5. J. Van der Lubbe, "Basic Methods of Cryptography" (Complementaria).
6. Pieprzyk, J., Hardjono, T., Seberry, J., "Fundamentals of Computer Security". (Complementaria)
7. N. Koblitz, "A Course in Number Theory and Cryptography" (Complementaria específica de Teoría de Números).
8. Ramanujachary Kumanduri, Cristina Romero, "Number Theory with Computer Applications". (Complementaria específica de Teoría de Números)
9. "Introducción a la Criptografía". Caballero, Pino. Ra-Ma, TextosUniversitarios (Complementaria).
10. Simon Singh, "Los códigos secretos". (Complementaria, divulgación).
11. Simon Singh, "The Code Book. " (Complementaria, divulgación).
12. Joan Daemen, Vicent Rijmen, "The design of Rijndael AES-The Advanced Encryption Standard". (Complementaria AES).

Nota: no se recomienda a los estudiantes comprar ningún libro, hasta haber comparado su contenido con el programa y revisado previamente en la biblioteca.

2. Métodos docentes

La metodología utilizada en el desarrollo de la actividad docente incluye los siguientes tipos de actividades:

***Clases de teoría:**

Actividad del profesor

Clases expositivas simultaneadas con la realización de programas y ejercicios. Se utilizará la pizarra, combinada con la explicación en formato electrónico cuya ejecución se visualizará en la pantalla de la clase cuando se requiera.

Actividad del estudiante:

Actividad presencial: Toma de apuntes, participación activa en clase respondiendo a las cuestiones planteadas. Resolución de los ejercicios propuestos y escritura de pequeños programas durante el desarrollo de las clases.

Actividad no presencial: lectura del material bibliográfico y de apoyo, estudio de la materia y realizaciones de los cuestionarios planteados en la plataforma Moodle.

***Clases de problemas/ejercicios en aula:**

Actividad del profesor

Primera parte expositiva, una segunda parte de supervisión y asesoramiento en la resolución de los problemas por parte del alumno y una parte final de análisis del resultado y generalización a otros tipos de problemas. Se utilizará la pizarra y el proyector del aula para visualizar los algoritmos o programas propuestos.

Actividad del estudiante:

Actividad presencial: Participación activa en la resolución de los ejercicios, diseño y escritura de los programas y en el análisis de la ejecución.

Actividad no presencial: Realización de ejercicios y programas, planteados en clase o a través de la plataforma Moodle. Estudio, generalización y planteamiento de modificaciones que permitan la optimización de los programas.

***Tutorías en aula:**

Actividad del profesor:

Tutorización a toda la clase o en grupos de alumnos reducidos (8-10) con el objetivo de resolver dudas comunes plantadas por los alumnos a nivel individual o en grupo, surgidas a partir de cuestiones/ejercicios/programas señalados en clase para tal fin y orientarlos en la realización de los mismos.

Actividad del estudiante:

Actividad presencial: Planteamiento de dudas individuales o en grupo y enfoque de posibles soluciones a las tareas planteadas.

Actividad no presencial: Estudio de las tareas marcadas y debate de las soluciones planteadas en el seno del grupo.

***Prácticas:**

Actividad del profesor:

Asignar una práctica/proyecto a cada grupo de trabajo y explicar la práctica asignada a cada grupo de trabajo al comienzo de la sesión de prácticas. Supervisar el trabajo de los grupos de trabajo en el laboratorio. Suministrar el guión de prácticas a completar en el laboratorio.

Se utilizan el método expositivo tanto en tutorías como en el laboratorio con cada grupo de trabajo. Los medios utilizados son los entornos de programación editores, compiladores y los ordenadores del propio laboratorio para la ejecución y análisis de los programas realizados.

Actividad del estudiante:

Actividad presencial: Planteamiento inicial, previo al desarrollo de la práctica, sobre información contenida en el enunciado. Debate en el seno del grupo sobre el planteamiento de la solución óptima. Al finalizar la práctica se entrega un informe explicando el desarrollo de la práctica y los programas desarrollados y, además, se debe ejecutar con el profesor presente, quien hará las preguntas oportunas a cada miembro del grupo para calificar de forma individual la práctica.

Actividad no presencial: Profundizar en el enunciado de la práctica y plantear el diagrama de flujo óptimo para la resolución de la misma. Redacción del informe de la práctica.

3. Tiempo de trabajo del estudiante

		Nº de horas	Porcentaje
Presencial	Clases teóricas	42 h (28%)	74 h (49.3%)
	Clases prácticas	26 h (17.3%)	
	Realización de pruebas escritas parciales y final	6 h (4%)	
No presencial	Estudio semanal regulado	18 h (12%)	76 h (50.7%)
	Realización de actividades prácticas	20 h (13.3%)	
	Preparación del examen (convocatoria ordinaria)	16 h (10.7%)	
	Preparación del examen (convocatoria extraordinaria)	22 h (14.7%)	
Carga total de horas de trabajo: 25 horas x 6 ECTS		**150 h**	

4. Métodos de evaluación y porcentaje en la calificación final

- Ambas partes, teoría y prácticas se puntúan sobre 10 puntos.
- La nota final de la asignatura se obtiene de las notas de teoría y prácticas por medio de la ecuación:

Calificación: 0.3*Prácticas + 0.7*Teoría

- Para aprobar la asignatura es obligatorio obtener una nota mayor o igual a 5 puntos, tanto en la parte de teoría como en las prácticas. En caso contrario, la nota final en actas será

Calificación: (0,3*Mín(5,Prácticas) + 0,7*Mín(5,Teoría))

La nota correspondiente a la parte de Teoría es la que resulta de:

- ✓ La calificación de la prueba final (60%).
- ✓ La calificación de las pruebas/actividades/ejercicios intermedios (al menos dos) (40%).

La nota correspondiente a la parte de Teoría para el itinerario sin asistencia obligatoria corresponde únicamente a la prueba final (distinta a la de la trayectoria con asistencia obligatoria ya que abarca ejercicios relacionados con las actividades intermedias).

Las pruebas escritas, podrán incluir tanto cuestiones teóricas y ejercicios como el diseño y escritura de programas.

- La nota correspondiente a la parte de prácticas es la que resulta de realizar las prácticas programadas en el curso.
  - ✓ Para aprobar la parte práctica el estudiante deberá asistir, al menos, al 85% de las prácticas. En caso contrario deberá realizar un examen de prácticas consistente en una práctica de mayor complejidad a las realizadas en el laboratorio.
  - ✓ La calificación de la parte práctica tendrá en cuenta la calidad de los diseños realizados y el nivel de los resultados obtenidos. También se valorará la validez de los resultados obtenidos en cada uno de los apartados que se hayan establecido para su realización en los guiones de las prácticas.
- La nota de teoría se conserva (convalida) sólo para la convocatoria extraordinaria del mismo curso académico.
- La nota de prácticas se conserva (convalida) sólo para la convocatoria extraordinaria del mismo curso académico.
- Para aquellos estudiantes que deban hacer uso de la **convocatoria extraordinaria** de junio habrá un único examen de la parte de teoría. Además el mismo día del examen los estudiantes deberán presentar las prácticas de la asignatura con todas las partes optativas realizadas. La ponderación de las dos partes se hará de acuerdo con la misma expresión utilizada en la convocatoria ordinaria.

ATENCIÓN: Cualquier copia descubierta que se haya realizado a lo largo del curso, tanto en cualquiera de las actividades de teoría desarrolladas, como en cualquiera de los apartados de las prácticas, serán penalizadas con rigor.

5. Cronograma

Semana	Contenido	Horas presenciales	Horas no presenciales
1	- Presentación y motivación de la asignatura, descripción del programa, normativa y los métodos de evaluación, descripción de la plataforma Moodle. - **Unidad 1 Introducción criptografía y seguridad informática. Temas 1.1 - 1.5** -Hoja 1 de problemas	3	2 Trabajo del estudiante: Lectura de las normativas de teoría y prácticas. Familiarización con el entorno Moodle. Lectura del material propuesto sobre la Unidad 1. Realización de los ejercicios propuestos.
2	- **Unidad 2 Métodos clásicos de cifrado y criptoanálisis. Temas 2.1, 2.2.1 - 2.2.5**	3	2 Trabajo del estudiante: Lectura de material propuesto sobre la Unidad 2. Realización de los ejercicios propuestos.
3	- **Unidad 2 Métodos clásicos de cifrado y criptoanálisis. Temas 2.2.6 - 2.2.7, 2.3** - Práctica 1	5	3 Trabajo del estudiante: Lectura de material propuesto sobre la Unidad 2. Realización de los ejercicios propuestos. Realización de Práctica 1.
4	- **Unidad 3 Criptografía teórica: cifrado perfecto y distancia de unicidad. Tema 3.1 - 3.3** - Hoja 2 de problemas - Práctica 1	5	3 Trabajo del estudiante: Lectura de material propuesto sobre la Unidad 3. Realización de los ejercicios propuestos. Realización de Práctica 1.
5	- **Unidad 3 Criptografía teórica: cifrado perfecto y distancia de unicidad. Tema 3.4 - 3.6** - Práctica 1	5	3 Trabajo del estudiante: Lectura de material propuesto sobre la Unidad 3. Realización de los ejercicios propuestos. Realización de Práctica 1.
6	- **Unidad 4 Criptografía simétrica. Tema 4.1, 4.2.1 - 4.2.3** - Hoja 3 de problemas - Práctica 1	5	3 Trabajo del estudiante: Lectura de material propuesto sobre la Unidad 4. Realización de los ejercicios propuestos. Realización de Práctica 1

Semana	Contenido	Horas presenciales	Horas no presenciales
7	- **Unidad 4 Criptografía simétrica. Tema 4.2.4 - 4.2.7** - Hoja 3 de problemas - Práctica 2	5	3 Trabajo del estudiante: Lectura de material propuesto sobre la unidad 4. Realización de los ejercicios propuestos. Entrega Práctica 1 Realización de Práctica 2.
8	- **Unidad 4 Criptografía simétrica. Tema 4.3.1 - 4.3.4** - Práctica 2	5	3 Trabajo del estudiante: Lectura de material propuesto sobre la unidad 4. Realización de los ejercicios propuestos. Realización de Práctica 2.
9	- **Unidad 4 Criptografía simétrica. Tema 4.3.5 - 4.3.8** - Práctica 2	5	3 Trabajo del estudiante: Lectura de material propuesto sobre la unidad 4. Realización de los ejercicios propuestos. Realización de Práctica 2.
10	- **Unidad 5 Criptografía publica. Tema 5.1 - 5.3.4** - Práctica 2 - Hoja 4 de problemas	5	3 Trabajo del estudiante: Lectura de material propuesto sobre la unidad 5. Realización de los ejercicios propuestos. Realización de Práctica 2.
11	- **Unidad 5 Criptografía publica. Tema 5.3.5 - 5.3.9** - Práctica 3	5	3 Trabajo del estudiante: Lectura del material propuesto sobre la Unidad 5. Realización de los ejercicios propuestos. Entrega Práctica 2. Realización de Práctica 3.
12	**- Unidad 6 Seguridad informática de protocolos: Mac y Hash. Tema 6.1 - 6.3** - Práctica 3	5	3 Trabajo del estudiante: Lectura del material propuesto sobre la Unidad 6. Realización de los ejercicios propuestos. Realización de Práctica 3.
13	**- Unidad 6 Seguridad informática de protocolos: Mac y Hash. Tema 6.4 - 6.5** - Práctica 3	5	3 Trabajo del estudiante: Lectura del material propuesto sobre la Unidad 6. Realización de los ejercicios propuestos. Realización de Práctica 3.

Semana	Contenido	Horas presenciales	Horas no presenciales
14	**- Intensificación**	5	1 Trabajo del estudiante: Resolución de los ejercicios propuestos. Entrega de Práctica 3.
	Examen Final	3	16h