

**PROGRAMA DE POSTGRADO MATEMÁTICAS  
 MASTER EN MATEMÁTICAS  
 DOCTORADO EN MATEMÁTICAS  
 DATOS BÁSICOS DEL CURSO**

Se aconseja que se rellene el documento protegido.

<b>Nombre del Curso:</b>
Criptografía y seguridad de sistemas informáticos.
<b>Código del curso (ver listado de cursos, tres dígitos):</b>
403
<b>Núm. ECTS:</b>
4
<b>Ubicación (Universidad del profesor responsable):</b>
Universidad de Granada

<b>Nombre del profesor responsable 1:</b>	
Fco. Javier Lobillo	
<b>Departamento:</b>	
Álgebra.	
<b>Área de Conocimiento:</b>	
Álgebra.	
<b>Localización del Despacho (Facultad, Escuela, etc.):</b>	
E. T. S. Ingeniería Informática, 2ª planta, despacho 13	
<b>e-mail:</b>	<b>URL web:</b>
jlobillo@ugr.es	<a href="http://www.ugr.es/~jlobillo">http://www.ugr.es/~jlobillo</a>
<b>Universidad:</b>	<b>Teléfono:</b>
Universidad de Granada	958 240 826

<b>Nombre del profesor responsable 2:</b>	
Blas Torrecillas	
<b>Departamento:</b>	
Álgebra y Análisis Matemático	
<b>Área de Conocimiento:</b>	
Álgebra.	
<b>Localización del Despacho (Facultad, Escuela, etc.):</b>	
<b>e-mail:</b>	<b>URL web:</b>
btorreci@ual.es	<a href="http://www.ual.es/~btorreci">http://www.ual.es/~btorreci</a>
<b>Universidad:</b>	<b>Teléfono:</b>
Universidad de Almería	950 015029

**1. Descriptores del curso:**  
 Criptografía simétrica y asimétrica. Firma Digital. Funciones hash. Criptosistemas basados en curvas elípticas. Certificación digital. Protocolos.

**2. Recomendaciones.**  
 Es necesario dominar la aritmética modular. Recomendable algunas nociones de geometría de curvas. Muy conveniente conocimientos de programación.

**3. Objetivos:**  
 Que el alumno conozca los principales algoritmos y técnicas utilizadas en criptografía. Que sea capaz de implementar y utilizar en entornos reales los protocolos y algoritmos empleados. Que el alumno sea capaz de configurar un servidor web seguro.

**4. Estructura (en horas de trabajo del estudiante):**

Clases de teoría:	12	
Clases de problemas:	4	
Clases prácticas en aula de informática:	8	
Seminarios y exposiciones:	4	
Trabajo en grupos reducidos:	<b>0</b>	
Total presencial:		<b>28</b>
Exámenes:	4	
Preparación de trabajos académicamente dirigidos y otras actividades:	20	
Estudio de clases presenciales:	<b>48</b>	
Total no presencial:		<b>72</b>
<b>Trabajo total del estudiante: 100,0 horas.</b>		

**5. Técnicas docentes (Metodología).**

**5.1. Técnicas docentes utilizadas:**

Sesiones académicas de teoría.  
 Sesiones académicas de problemas.  
 Sesiones prácticas en el aula de informática.  
 Seminarios, exposiciones y debates.  
 Trabajo en grupos reducidos.  
 Otras: Especificar.  
 Otras: Especificar.

**5.2. Desarrollo y justificación:**

En esta asignatura se pretende que el alumno conozca algunos de los algoritmos y sistemas criptográficos más estandarizados y que los aplique a soluciones reales en entornos informáticos. Por ello por cada hora de teoría habrá una hora de problemas o de prácticas en el laboratorio de ordenadores, dependiendo del contenido teórico. En principio las primeras semanas deben contener más contenido teórico, dejando las últimas para trabajos completamente prácticos. Es conveniente que el alumno asista a las exposiciones de los compañeros, aunque no es necesario.

**6. Programa del curso:**

1. Conceptos básicos.
  - 1.1 Criptografía simétrica: DES, IDEA, AES, y cifrados de flujo.
  - 1.2 Criptografía asimétrica: RSA, Diffie-Hellman y ElGamal.
  - 1.3 Criptosistemas basados en curvas elípticas.
  - 1.4 Comparación de criptosistemas.
2. Firma Digital.
  - 2.1 Características generales.
  - 2.2 Funciones hash.
  - 2.3 Esquemas basados en criptosistemas asimétricos.
  - 2.4 DSA.
3. Certificados digitales.
  - 3.1 Estructura general
  - 3.2 Autoridades de Certificación.
  - 3.3 Listas de revocación.
  - 3.4 Estándar X509.
  - 3.5 Certificación de sitios web.
4. Protocolos.
  - 4.1 Secreto compartido.
  - 4.2 Protocolos de conocimiento cero.
  - 4.3 Implementación de protocolos de seguridad.

## 7. Bibliografía.

Brassard, Guiles: "Modern Cryptography, a tutorial", Springer-Verlag, 1988.  
Dawson; Golic: "Cryptography: policy and algorithms", 1996.  
Koblitz, Neal: "A course in number theory and cryptography", Springer-Verlag, 1979.  
Manuel Lucena López: "<http://www.di.ujaen.es/~mlucena/lcripto.html>" "Criptografía y Seguridad en Computadores", Universidad de Jaén.  
D.R. Stinson: "Cryptography: Theory & Practice", CRC 1995

## 8. Evaluación.

### 8.1. Técnicas de evaluación utilizadas:

Examen teórico-práctico.  
Trabajos desarrollados durante el curso.  
Participación activa en las sesiones académicas.  
Controles periódicos de adquisición de conocimientos.  
Examen de prácticas en aula de informática.  
Otras: Especificar.  
Otras: Especificar.

### 8.2. Criterios de evaluación y calificación:

Las prácticas serán el 40% de la calificación final. El examen teórico un 25%. Trabajos un 20 %. Controles un 10%. Participación un 5%.