

DATOS IDENTIFICATIVOS				
Seguridad de la información				
Asignatura	Seguridad de la información			
Código	V05M175V01102			
Titulacion	Máster Universitario en Ciberseguridad			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	6	OB	1	1c
Lengua Impartición	Inglés			
Departamento				
Coordinador/a	Fernández Veiga, Manuel			
Profesorado	Fernández Veiga, Manuel Gestal Pose, Marcos Pérez González, Fernando			
Correo-e	mveiga@det.uvigo.es			
Web	http://faitic.uvigo.es			
Descripción general	En esta asignatura se estudian las técnicas de criptografía y criptoanálisis, la generación de números y funciones aleatorias, los métodos de integridad de mensajes, el cifrado autenticado, el cifrado asimétrico, los métodos de privacidad y anonimato de la información, los esquemas de computación segura y la estenografía. Todas las anteriores son herramientas básicas para la protección de la información en redes y sistemas			

Competencias	
Código	
A2	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio
A5	Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo
C1	Conocer, comprender y aplicar los métodos de criptografía y criptoanálisis, los fundamentos de identidad digital y los protocolos de comunicaciones seguras
C4	Comprender y aplicar los métodos y técnicas de ciberseguridad aplicables a los datos, los equipos informáticos, las redes de comunicaciones, las bases de datos, los programas y los servicios de información
C10	Conocer los fundamentos matemáticos de las técnicas criptográficas y comprender su evolución y tendencias futuras.

Resultados de aprendizaje	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Conocer los conceptos de cifrado Shannon, seguridad perfecta y seguridad semántica	C1 C10
Conocer y saber utilizar los métodos de cifrado en flujo	C1 C4 C10
Conocer y saber utilizar los métodos de cifrado en bloque, las funciones seudoaleatorias y los estándares DES y AES	C1 C4 C10
Comprender, saber construir y saber utilizar las funciones de hash, las funciones hash universales y con ellas los mecanismos de integridad de la información	C1 C4 C10
Comprender y saber utilizar los principios del cifrado asimétrico y los esquemas criptigráficos Diffie-Hellman, RSA y ElGamal. Comprender y saber utilizar las firmas digitales	C1 C4 C10

Conocer los fundamentos de técnicas de cifrado avanzado: cifrado con curvas elípticas y sobre retículos	A2 A5 C1 C4 C10
Conocer y saber utilizar los protocolos de intercambio de claves y de comunicaciones interactivas seguras	A5 C1 C4 C10
Conocer, comprender y saber utilizar las técnicas de anonimización de datos	A5 C1 C4 C10
Conocer, comprender y saber aplicar las técnicas básicas de esteganografía, marcado digital y forenses	A2 A5 C1 C4 C10
Conocer y comprender las ideas básicas de la computación segura	A2 A5 C1 C4 C10

Contenidos

Tema	
1. Cifrado	Cifrado de Shannon Seguridad perfecta Seguridad semántica y computacional
2. Cifrado en flujo	Generadores pseudo aleatorios simples y compuestos Ataques Casos de estudio
3. Cifrado en bloques	Cifrado en bloques. Seguridad DES. AES Funciones pseudoaleatorias Construcción de PRF y cifrado en bloques
4. Integridad	Códigos de autenticación e integridad. Definición de seguridad. MAC con claves. Funciones pseudoaleatorias y MAC. Funciones hash. Hashing universal y hashing resistente a colisiones. Casos de estudio
5. Cifrado autenticado	Definición. Composición. Ataques. ejemplos y casos de estudio
6. Cifrado con clave pública	Definición. Seguridad semántica. Funciones de una dirección. Esquemas RSA, ElGamal, Diffie-Hellman. Firmas digitales. Casos de estudio
7. Cifrado avanzado	Cifrado sobre curvas elípticas. Retículos. Cifrado sobre retículos. RLWE. Ataques cuánticos. Computación homomórfica
8. Protocolos de identificaciín	Definición. Contraseñas (de un solo uso). Challenge-response. Sigma-protocolos. Esquemas de Okamoto y Schnorr. Casos de estudio
9. Anonimización	Definición. t-integridad, divergencia. Análisis. Casos de estudio
10. Esteganografía y watermarking	Definiciones. Marcado de agua mediante espectro ensanchado. Codificación de papel sucio. Forensía digital.
11. Computación segura	Funciones computables. Computación segura a dos vías. Computación segura a varias vías. Computación interactiva segura. Computación homomórfica. Aplicaciones

Planificación

	Horas en clase	Horas fuera de clase	Horas totales
Resolución de problemas	0	24	24
Prácticas de laboratorio	18	36	54
Lección magistral	17	51	68
Examen de preguntas de desarrollo	2	0	2
Resolución de problemas y/o ejercicios	1	0	1
Proyecto	1	0	1

*Los datos que aparecen en la tabla de planificación son de carácter orientativo, considerando la heterogeneidad de alumnado

Metodologías

	Descripción

Resolución de problemas	Los estudiantes resolverán problemas y ejercicios sobre los contenidos de las lecciones. Entrega por escrito y corrección. Con esta metodología se trabajan las competencias CB2, CB4, CB5, CE1, CE 4, CE10 y CT5.
Prácticas de laboratorio	Los estudiantes desarrollarán en el laboratorio prácticas de seguridad de los datos y un proyecto de programación sobre cifrado, firma, anonimato o forenses digital. Las prácticas o proyectos serán supervisadas por los profesores. Con esta metodología se trabajan las competencias CB2, CB4, CB5, CE1, CE 4, CE10 y CT4.
Lección magistral	Exposición sistemática de los contenidos del curso: conceptos, resultados, algoritmos, ejemplos y casos de uso. Con esta metodología se trabajan las competencias CB2, CB4, CB5, CE1, CE 4, CE10 y CT5

Atención personalizada

Metodologías	Descripción
Lección magistral	Se dispensará atención individual a los estudiantes que precisen orientación para el estudio, explicación adicional sobre los contenidos de la disciplina, aclaración o guía sobre la resolución de problemas.
Resolución de problemas	Se atenderán individualmente las consultas sobre la resolución de problemas y ejercicios planteados en las clases o trabajados de forma autónoma
Prácticas de laboratorio	Se responderán individualmente las cuestiones relativas a las prácticas de laboratorio y al desarrollo del proyecto.

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje	
Examen de preguntas de desarrollo	Examen escrito. Resolución de cuestiones, problemas o ejercicios.	50	A2 A5	C1 C4 C10
Resolución de problemas y/o ejercicios	Resolución de cuestiones, problemas y ejercicios a lo largo del curso (2 o 3 cuestionarios). Entrega individual por escrito	20	A2 A5	C1 C4 C10
Proyecto	Desarrollo de un proyecto de implementación de un sistema de protección de información. Pruebas funcionales y de rendimiento	30	A2 A5	C1 C4 C10

Otros comentarios sobre la Evaluación

Se dejan a discreción de los alumnos dos métodos de evaluación alternativos en la asignatura: evaluación continua y evaluación única.

La evaluación continua consistirá en la realización de un examen final (50% de la calificación), el desarrollo de prácticas y proyecto (30% de la calificación) que se presentará antes del último día hábil anterior al periodo oficial de exámenes y en la entrega a lo largo del curso de ejercicios resueltos (20%). La evaluación única consistirá en la realización de un examen final escrito (60% de la calificación) y en el desarrollo de proyectos de ingeniería a escala (40% de la calificación) que se presentará antes del último día hábil anterior al periodo oficial de exámenes. Las pruebas escritas de las modalidades de evaluación única y continua no serán necesariamente iguales.

Los alumnos podrán optarán por una u otra modalidad de evaluación hasta la fecha del examen escrito del curso.

Quienes no superen la asignatura en la primera oportunidad de la convocatoria disponen de una segunda oportunidad al final del curso en la que se reevaluarán sus conocimientos con una prueba escrita o se reevaluará su proyecto si se hubiera mejorado o modificado éste. Los pesos de cada una de las pruebas (examen y proyecto) serán los mismos que en el periodo ordinario de evaluación conforme a la modalidad que se hubiese elegido.

La calificación de las pruebas solo surte efecto en el curso académico en que se obtengan, con independencia del itinerario de evaluación escogido.

Fuentes de información

Bibliografía Básica

D. Boneh, V. Shoup, **A graduate course in applied cryptography**, http://toc.cryptobook.us, 2018

Bibliografía Complementaria

O. Goldreich, **Foundation of cryptography, vol. I**, Cambridge University Press, 2007

O. Goldreich, **Foundation of cryptography, vol. ii**, Cambridge University Press, 2009

J. Katz, Y. Lindell, **Introduction to modern cryptography**, 2, CRC Press, 2015

A. Menezes, P. van Oorschot, S. Vanstone., **Handbook of applied cryptography**, CRC Press, 2001

C. Dwork, A. Roth, **The algorithmic foundations of differential privacy**, NOW Publishers, 2014

W. Mazurczyk, S. Wenzel, S. Zander, A. Houmansadr, K. Szczypiorski, **Information hiding in communications networks: Fundamentals, mechanisms, applications, and countermeasures**, Wiley, 2016

I. Cox, M. Miller, J. Bloom, J. Fridrich, T. Kolker, **Digital watermarking and steganography**, 2, Morgan Kaufmann, 2008

A. El-Gamal, Y. Kim, **Network Information Theory**, Cambridge University Press, 2011

Recomendaciones

Otros comentarios

La asignatura se imparte en inglés. Es recomendable aptitud para el razonamiento matemático.