



DATOS IDENTIFICATIVOS

Seguridade da información

Materia	Seguridade da información			
Código	V05M175V01102			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	6	OB	1	1c
Lingua de impartición	Inglés			
Departamento				
Coordinador/a	Fernández Veiga, Manuel			
Profesorado	Fernández Veiga, Manuel Gestal Pose, Marcos Vázquez Padín, David			
Correo-e	mveiga@det.uvigo.es			
Web	http://movi.uvigo.gal			
Descrición xeral	Nesta materia se estúdanse as técnicas de criptografía e criptoanálise, a xeración de números e funcións aleatorias, os métodos de integridade de mensaxes, o cifrado autenticado, o cifrado asimétrico, os métodos de privacidade e anonimato da información, os esquemas de computación segura e a esteganografía. Todas as anteriores son ferramentas básicas para a protección da información en redes e sistemas.			

Competencias

Código	
A2	Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos máis amplos (ou multidisciplinares) relacionados coa súa área de estudo
A5	Que os estudantes posúan as habilidades de aprendizaxe que lles permitan continuar estudando dun modo que haberá de ser en gran medida autodirixido ou autónomo
C1	Coñecer, comprender e aplicar os métodos de criptografía e criptoanálisis, os fundamentos de identidade dixital e os protocolos de comunicacións seguras.
C4	Comprender e aplicar os métodos e técnicas de ciberseguridade aplicables ós datos, os equipos informáticos, as redes de comunicacións, as bases de datos, os programas e os servizos de información
C10	Coñecer os fundamentos matemáticos das técnicas criptográficas e comprender a súa evolución e tendencias futuras.

Resultados de aprendizaxe

Resultados previstos na materia	Resultados de Formación e Aprendizaxe
Coñecer os conceptos de cifrado Shannon, seguridade perfecta e seguridade semántica	C1 C10
Coñecer e saber utilizar os métodos de cifrado en fluxo	C1 C4 C10
Coñecer e saber utilizar os métodos de cifrado en bloque, as función pseudoaleatorias e os estándares DES e AES	C1 C4 C10
Comprender, saber construír e saber utilizar as funcións de hash, as funcións hash universais e con elas os mecanismos de integridade da información	C1 C4 C10
Comprender e saber utilizar os principios do cifrado de chave pública e os correspondentes esquemas criptográficos: Diffie-Hellman, RSA, ElGamal. Comprender e saber utilizar as firmas dixitais	C1 C4 C10

Coñecer os fundamentos das técnicas de cifrado avanzado: cifrado con curvas elípticas e cifrado sobre retículas	A2 A5 C1 C4 C10
Coñecer e saber utilizar os protocolos de intercambio de claves e de comunicación interactivas seguras	A5 C1 C4 C10
Coñecer, comprender e saber utilizar as técnicas de anonimización dos datos	A5 C1 C4 C10
Coñecer, comprender e saber aplicar as técnicas básicas de esteganografía, marcados de auga e forense dixital	A2 A5 C1 C4 C10
Coñecer e comprender as ideas básicas da computación segura	A2 A5 C1 C4 C10

Contidos

Tema		
1. Cifrado	Cifrado Shannon. Seguridade perfecta. Seguridade semántica. Seguridade baseada na teoría da información. A canle wiretap	
2. Cifrado en fluxo	Xeneradores pseudoaleatorios simples e compostos. Ataques. Casos de estudo	
3. Cifrado en bloques	Cifrado en bloques. Seguridade. DES. AES. Funcións pseudoaleatorias. Contrución de PRF e cifrado en bloques.	
4. Integridade	Códigos de autenticación e integridade de mensaxes. Definición de seguridade. MAC con claves. Funcións pseudoaleatorias e MAC. Funcións hash. Hashing universal e resistente a colisión. Casos de estudo	
5. Cifrado autenticado	Definición. Composición. Ataques. Exemplos e casos de estudo	
6. Cifrado con chave pública	Definición. Seguridade semántica. Funcións de dirección. Esquemas RSA, ElGamal, Diffie-Hellman. Firmas dixitais. Casos de estudo.	
7. Cifrado avanzado	Cifrado sobre curvas elípticas. Retículas e cifrado sobre retículas. RLWE. Ataques cuánticos. Cifrado homomórfico	
8. Protocolos de identificación	Definición. Contraseñas (dun só uso). Challenge.response. Sigma-protocolos. Esquemas de Okamoto e Schnorr. Casos de estudo.	
9. Anonimización	Definición. t-integridade, diverxencia, análise	
10. Ocultación de datos e forense dixital	Definicións. Marcado de auga mediante espectro ensanchado. Codificación de papel sucio. Forense dixital.	
11. Computación segura	Funcións computables. Computación segura a dúas vías e a varias vías. Computación interactiva. Computación homomórfica. Aplicacións.	
1. Cifrado	Cifrado Shannon. Seguridade perfecta. Seguridade semántica. Seguridade baseada na teoría da información. A canle wiretap	

Planificación

	Horas na aula	Horas fóra da aula	Horas totais
Resolución de problemas	0	24	24
Prácticas de laboratorio	18	36	54
Lección maxistral	17	51	68
Exame de preguntas de desenvolvemento	2	0	2
Resolución de problemas e/ou exercicios	1	0	1
Proxecto	1	0	1

*Os datos que aparecen na táboa de planificación son de carácter orientador, considerando a heteroxeneidade do alumnado.

Metodoloxía docente

	Descrición
Resolución de problemas	Os estudantes resolverán problemas e exercicios sobre o material do curso.
	Con esta metodoloxía trabállanse as competencias CB2, CB4, CB5, CE1, CE4, CE10 e CT5.

Prácticas de laboratorio	Os estudantes desenvolverán no laboratorio prácticas de seguridade da información con ordenador, e un proxecto de programación sobre cifrado, firma, anonimato ou forensia. As prácticas e proxectos estarán supervisados polos profesores.
	Con esta metodoloxía trabállanse as competencias CB2, CB4, CB5, CE1, CE4, CE10 e CT4.
Lección maxistral	Exposición sistemática dos contidos do curso: conceptos, resultados, algoritmos, exemplos e casos de uso.
	Con esta metodoloxía trabállanse as competencias CB2, CB4, CB5, CE1, CE4, CE10 e CT5.

Atención personalizada

Metodoloxías	Descrición
Lección maxistral	Ofrecerase atención individual aos estudantes que precisen orientación para o estudo, explicacións adicionais sobre os contidos da disciplina, aclaración ou guía sobre resolución de problemas
Resolución de problemas	Atenderanse individualmente as consultas sobre a resolución de problemas e exercicios planteados nas clases ou traballados de xeito autónomo
Prácticas de laboratorio	Responderanse individualmente as cuestións relativas ás prácticas de laboratorio e ao desenvolvemento do proxecto

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe	
Exame de preguntas de desenvolvemento	Exame escrito. Resolución de cuestións, exercicios ou problemas.	50	A2 A5	C1 C4 C10
Resolución de problemas e/ou exercicios	2 ou 3 conxuntos de problemas, exercicios ou cuestións ao longo do curso, para resolución individual polos estudantes. Entrega por escrito	25	A2 A5	C1 C4 C10
Proxecto	Desenvolvemento dun proxecto de implementación dun sistema de protección da información. Probas funcionais e de rendemento.	25	A2 A5	C1 C4 C10

Outros comentarios sobre a Avaliación

Déixanse a discreción dos alumnos dous métodos de avaliación alternativos na materia: avaliación continua e avaliación única.

A avaliación continua consistirá na realización dun exame final (50% da cualificación) e no desenvolvemento de proxectos de enxeñaría a escala (25% da cualificación) que se presentará antes do último día hábil anterior ao período oficial de exames. A avaliación única consistirá na realización dun exame final escrito (60% da cualificación) e no desenvolvemento de proxectos de enxeñaría a escala (40% da cualificación) que se presentará antes do último día hábil anterior ao período oficial de exames. As probas escritas das modalidades de avaliación única e continua non serán necesariamente iguais.

Os alumnos optarán por unha ou outra modalidade de avaliación ata a data do exame escrito do curso.

Quen non superen a materia na primeira oportunidade da convocatoria dispoñen dunha segunda oportunidade ao final do curso na que se reavaliarán os seus coñecementos cunha proba escrita ou se reavaliará o seu proxecto se se mellorou ou modificou. Os pesos de cada unha das probas (exame e proxecto) serán os mesmos que no período ordinario de avaliación conforme á modalidade que se elixiu.

A cualificación das probas só fornece efecto no curso académico en que se obteñan, con independencia do itinerario de avaliación escollido.

Bibliografía. Fontes 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

Recomendacións

Outros comentarios

A materia impártese en inglés. É recomendable ser capacidade para o razoamento matemático
