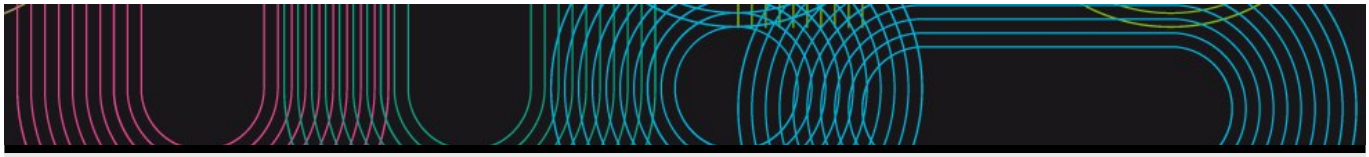

DATOS IDENTIFICATIVOS				
Seguridade da información				
Materia	Seguridade da información			
Código	V05M175V11108			
Titulación	Máster Universitario en Ciberseguridade			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OB	1	1c
Lingua de impartición	Inglés			
Departamento				
Coordinador/a	Fernández Veiga, Manuel			
Profesorado	Fernández Veiga, Manuel Gestal Pose, Marcos Pérez González, Fernando			
Correo-e	mveiga@det.uvigo.es			
Web	http://moovi.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.			

Resultados de Formación e Aprendizaxe
Código

Resultados previstos na materia	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe

Contidos	
Tema	
1. Cifrado	Cifrado Shannon. Seguridade perfecta. Seguridade semántica. Seguridade baseada na teoría da información. A canle wiretap
2. Cifrado en fluxo	Xeneradores seudoaleatorios simples e compostos. Ataques. Casos de estudo
3. Cifrado en bloques	Cifrado en bloques. Seguridade. DES. AES. Funcións seudoaleatorias. Contrución de PRF e cifrado en bloques.
4. Integridade	Códigos de autenticación e integridade de mensaxes. Definición de seguridade. MAC con chaves. Funcións seudoaleatorias 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 ducha dirección. Esquemas RSA, ElGamal, Diffie-Hellman. Firmas dixitais. Casos de estudo
7. Cifrado avanzado	Cifrado sobre curvas elípticas. Retículos e cifrado sobre retículas. RLWE. Ataques cuánticos. Cifrado homomórfico
8. Protocolos de identificación	Definición. Contraseñas (dun so uso). Challenge.response. Sigmaprotocolos. Esquemas de Okamoto e Schnorr. Casos de estudo
9. Anonimización	Definición. t-integridade, diverxencia, análise
10. Ocultación de datos e forensic dixital	Definicións. Marcado de auga mediante espectro ensanchado. Codificación de papel sucio. Forensia dixital.

11. Computación segura	Funcións computables. Computación segura a dúas vías e a varias vías. Computación interactiva. Computación homomórfica. Aplicacións.

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	2	0	2

*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.
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 proyectos estarán supervisados polos profesores.
Lección maxistral	Exposición sistemática dos contidos do curso: conceptos, resultados, algoritmos, exemplos e casos de uso.

Atención personalizada	
Metodoloxías	**Descrición**
Resolución de problemas	Atenderanse individualmente as consultas sobre a resolución de problemas e ejercicios planteados las clases ou traballados de xeito autónomo. O horario de tutorías pode consultarse en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
Prácticas de laboratorio	Responderanse individualmente as cuestión relativas ás prácticas de laboratorio e ao desenvolvemento dos proxectos O horario de tutorías pode consultarse en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga
Lección maxistral	Ofrecerase atención individual aos estudantes que precisen orientación para o estudo, explicacións adicionáis sobre os contados da disciplina, aclaración ou guía sobre resolución de problemas. O horario de tutorías pode consultarse en https://www.uvigo.gal/es/universidad/administracion-personal/pdi/manuel-fernandez-veiga

Avaliación			
	Descrición	Cualificación	Resultados de Formación e Aprendizaxe
Resolución de problemas	4 conxjuntos de problemas, exercicios ou cuestións ao longo do curso, para resolución individual polos estudantes. Entrega por escrito	30	
Prácticas de laboratorio	Desenvolvemento de proxectos de implementación dun sistema de protección da información. Probas funcionais e de rendemento.	30	
Exame de preguntas de desenvolvemento	Exame escrito. Resolución de cuestións, ejercicios ou problemas.	40	

Outros comentarios sobre a Avaliación

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

global.

A avaliación continua consistirá na realización dun exame final (40% da cualificación) e no desenvolvemento de proxectos

de enxeñaría a escala (30% da cualificación). A avaliación global consistirá na realización dun exame fina escrito (40% da cualificación) e no desenvolvemento de

proxectos de enxeñaría a escala (dous, 30% da cualificación cada un) que se presentará antes do último día hábil anterior

ao período

oficial de exames. As probas escritas das modalidades de avaliación global 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 oportunidade ordinaria da convocatoria dispoñen dunha convocatoria extraordinaria 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, 2021

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**, 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