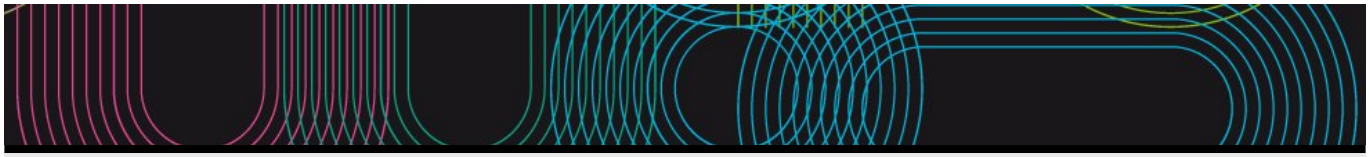

DATOS IDENTIFICATIVOS				
Seguridade Multimedia				
Materia	Seguridade Multimedia			
Código	V05M145V01318			
Titulación	Máster Universitario en Enxeñaría de Telecomunicación			
Descritores	Creditos ECTS	Sinale	Curso	Cuadrimestre
	5	OP	2	1c
Lingua de impartición	Inglés			
Departamento	Teoría do sinal e comunicacións			
Coordinador/a	Pérez González, Fernando			
Profesorado	Pérez González, Fernando			
Correo-e	fperez@gts.uvigo.es			
Web	http://faitic.uvigo.es			
Descrición xeral	A seguridade multimedia é un tema cada vez máis importante dado que a maior parte da información que se intercambia hoxe en día en Internet é multimedia. As solucións de protección de datos tradicionais como a criptografía só poden solucionar o problema parcialmente, porque os contidos, unha vez descifrados, deixan de estar protexidos. Ademais, hai unha preocupación crecente sobre a integridade dos contidos multimedia: as ferramentas modernas de edición cuestionan a nosa confianza nos vídeos, imaxes ou audio. Afortunadamente, numerosos de grupos investigación e empresas abordaron estes problemas e propuxeron solucións enxeñosas. O presente curso presenta temas en seguridade multimedia, facendo énfase na criptografía, o marcado de auga, en análise dixital forense e o procesado de sinal no dominio cifrado. Impártese e evalúase en inglés. Os contidos están en inglés. Os alumnos poden participar nas clases e responder nos exames desexablemente en inglés, pero tamén é posible facelo en galego ou castelán.			

Competencias	
Código	
B4	CG4 Capacidade para o modelado matemático, cálculo e simulación en centros tecnolóxicos e de enxeñaría de empresa, particularmente en tarefas de investigación, desenvolvemento e innovación en todos os ámbitos relacionados coa Enxeñaría de Telecomunicación e campos multidisciplinais afíns.
B8	CG8 Capacidade para a aplicación dos coñecementos adquiridos e resolver problemas en ámbitos novos ou pouco coñecidos dentro de contextos máis amplos e mulitidisciplinais, sendo capaces de integrar coñecementos.
C31	CE37/OP7 Capacidade para modelar, operar, administrar, e afrontar o ciclo completo e empaquetamiento de redes, servizos e aplicacións considerando a calidade de servizo, os custes directos e de operación, o plan de implantación, supervisión, seguridade, escalado e mantemento, xestionando e asegurando a calidade no proceso de desenvolvemento

Resultados de aprendizaxe	
Resultados previstos na materia	Resultados de Formación e Aprendizaxe
Manexar os esquemas de protección da información máis avanzados	B4 B8 C31
Comprender as capacidades e limitacións dos distintos métodos	B4 B8 C31

Manexar o uso dos diferentes algoritmos nas distintas contornas de comunicacións multimedia que se poden expor actualmente.	B4 B8 C31
Comprender material técnico de forma autónoma.	B4 B8 C31

Contidos	
Tema	
Introdución a criptografía.	Aplicación a sistemas multimedia. Integración con codificación de fonte e de canle. Cifrado bloque e secuencial. Hashing e códigos MAC. Algoritmos específicos.
Sistemas de acceso condicional.	Requisitos. Historia e estado da arte. Deseño dun sistema de acceso condicional.
Compartición de segredos.	Sistema sinxelo de compartición de segredos. Criptografía visual.
Ocultación de datos e marcado de auga.	Conceptos básicos. Marcado de auga e ocultación de datos. Marcado de auga en espectro ensanchado. Marcado de auga mediante cuantificación. Aplicación a imaxes e vídeo.
Procesamento de sinal forense.	Detección e estimación de cuantificación. Detección e identificación de filtrado. Detección e estimación de remostreo. Balística de fontes.
Procesado de sinal no dominio cifrado.	Métricas e conceptos de privacidade. Cifrado homomórfico. Circuítos ilexibles. Representación de sinais e explosión de cifras. Aplicacións.

Planificación			
	Horas na aula	Horas fóra da aula	Horas totais
Sesión maxistral	14	28	42
Prácticas de laboratorio	9	42	51
Informes/memorias de prácticas	0	30	30
Probas de resposta longa, de desenvolvemento	2	0	2

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

Metodoloxía docente	
	Descrición
Sesión maxistral	O curso está estruturado en varios temas en seguridade multimedia, incluíndo criptografía, marcado de auga, forensía e procesado de sinal no dominio cifrado. Competencias: CG4, CG8, CE31
Prácticas de laboratorio	As prácticas de laboratorio cubrirán aspectos diferentes da ocultación de datos, marcado de auga e forensía. Isto permitirá que os estudantes implementen e expandan considerablemente algúns dos conceptos vistos nas clases. Competencias: CG4, CG8, CE31

Atención personalizada	
Metodoloxías	**Descrición**
Sesión maxistral	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse de forma presencial (durante a propia sesión maxistral, ou durante o horario establecido para tutorías). O horario de tutorías se establecerá ao principio do curso e se publicará na páxina web da asignatura.
Probas	**Descrición**

Informes/memorias de prácticas	Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse de forma presencial (durante as sesións de seguimento do traballo, ou durante o horario establecido para tutorías).

Avaliación

	Descrición	Cualificación	Resultados de Formación e Aprendizaxe	
Informes/memorias de prácticas	Informes das prácticas e traballo persoal adicional que empregue as técnicas vistas na aula. Avaliarase a calidade dos informes e a corrección dos resultados. Os informes serán individuais ou colectivos, dependendo da unidade que realizou cada práctica.	70	B4 B8	C31
Probas de resposta longa, de desenvolvemento	Exame final con cuestións curtas sobre os contidos do curso.	30	B4 B8	C31

Outros comentarios sobre a Avaliación

Requírese unha puntuación mínima do 30% con respecto ao máximo posible no exame final para aprobar a materia.

Naqueles casos en que o alumno decida non realizar as tarefas de avaliación continua, a nota final basearase exclusivamente no exame con cuestións sobre a materia. Isto aplica tamén á segunda convocatoria.
En caso de informes colectivos, deberase explicitar a contribución de cada alumno ao mesmo, e a avaliación será individualizada, en función da devandita contribución.
Unha vez que o alumno entrega algún dos entregables, está automaticamente decidindo ser avaliado de forma continua.
Calquera alumno decide ser avaliado de forma continua, terá unha nota final, independentemente de se realiza o exame final ou non.
As tarefas de avaliación continua non poden repetirse despois das súas correspondentes datas de entrega, e son válidas só para o curso actual.
No caso de detección de plaxio nalgún dos traballos/probas realizadas a cualificación final da asignatura será de suspenso (0) e os profesores comunicarán a dirección da escola o asunto para que tome as medidas que considere oportunas.
Asemade, os profesores comunicarán a dirección da escola cualquera conducta contraria a ética por parte dos alumnos, existindo a posibilidade de que aquela tome as medidas oportunas.

Bibliografía. Fontes de información

Cox, Miller, Bloom, Fridrich, Kalker, **Digital Watermarking and Steganography**, 2nd,

Troncoso-Pastoriza, Perez-Gonzalez, **Secure Signal Processing in the Cloud: enabling technologies for privacy-preserving multimedia cloud processing**, Signal Processing Magazine,

A.J. Menezes, **Handbook of Applied Cryptography**, 1996,

A. Piva, **An Overview of Image Forensics**, Signal Processing,

Recomendacións

Materias que se recomenda ter cursado previamente

Procesado Estatístico do Sinal/V05M145V01303