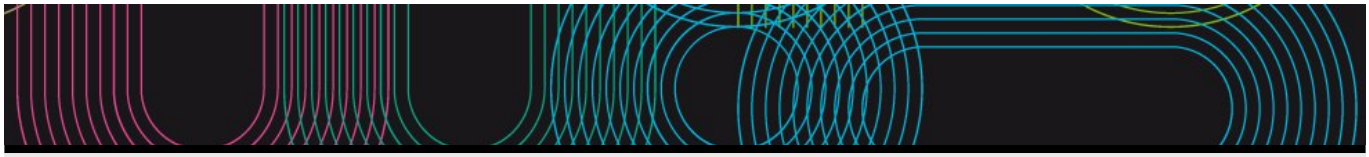

DATOS IDENTIFICATIVOS				
Seguridad Multimedia				
Asignatura	Seguridad Multimedia			
Código	V05M145V01318			
Titulacion	Máster Universitario en Ingeniería de Telecomunicación			
Descriptores	Creditos ECTS	Seleccione	Curso	Cuatrimestre
	5	OP	2	1c
Lengua Impartición	Inglés			
Departamento	Teoría de la señal y comunicaciones			
Coordinador/a	Pérez González, Fernando			
Profesorado	Pérez González, Fernando			
Correo-e	fperez@gts.uvigo.es			
Web	http://faitic.uvigo.es			
Descripción general	La seguridad multimedia es un tema cada vez más importante dado que la mayor parte de la información que se intercambia hoy en día en Internet es multimedia. Las soluciones de protección de datos tradicionales como la criptografía sólo pueden solucionar el problema parcialmente, porque los contenidos, una vez descifrados, dejan de estar protegidos. Además, hay una preocupación creciente sobre la integridad de los contenidos multimedia: las herramientas modernas de edición cuestionan nuestra confianza en los vídeos, imágenes o audio. Afortunadamente, numerosos de grupos investigación y empresas han abordado estos problemas y han propuesto soluciones ingeniosas. El presente curso presenta temas en seguridad multimedia, haciendo énfasis en la criptografía, el marcado de agua, en análisis digital forense y el procesado de señal en el dominio cifrado. Se imparte y se evalúa en inglés. Los contenidos están en inglés. Los alumnos pueden participar en las clases y responder en los exámenes deseablemente en inglés, pero también es posible hacerlo en gallego o castellano.			

Competencias	
Código	
B4	CG4 Capacidad para el modelado matemático, cálculo y simulación en centros tecnológicos y de ingeniería de empresa, particularmente en tareas de investigación, desarrollo e innovación en todos los ámbitos relacionados con la Ingeniería de Telecomunicación y campos multidisciplinares afines.
B8	CG8 Capacidad para la aplicación de los conocimientos adquiridos y resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y mulitidisciplinares, siendo capaces de integrar conocimientos.
C31	CE37/OP7 Capacidad para modelar, operar, administrar, y afrontar el ciclo completo y empaquetamiento de redes, servicios y aplicaciones considerando la calidad de servicio, los costes directos y de operación, el plan de implantación, supervisión, seguridad, escalado y mantenimiento, gestionando y asegurando la calidad en el proceso de desarrollo.

Resultados de aprendizaje	
Resultados previstos en la materia	Resultados de Formación y Aprendizaje
Manejar los esquemas de protección de la información más avanzados	B4 B8 C31
Comprender las capacidades y limitaciones de los distintos métodos	B4 B8 C31

Manejar el uso de los diferentes algoritmos en los distintos entornos de comunicaciones multimedia que se pueden plantear actualmente.	B4 B8 C31
Comprender material técnico de forma autónoma.	B4 B8 C31

Contenidos	
Tema	
Introducción a criptografía.	Aplicación a sistemas multimedia. Integración con codificación de fuente y de canal. Cifrado bloque y secuencial. Hashing y códigos MAC. Algoritmos específicos.
Sistemas de acceso condicional.	Requisitos. Historia y estado del arte. Diseño de un sistema de acceso condicional.
Compartición de secretos.	Sistema sencillo de compartición de secretos. Criptografía visual.
Ocultación de datos y marcado de agua.	Conceptos básicos. Marcado de agua y ocultación de datos. Marcado de agua en espectro ensanchado. Marcado de agua mediante cuantificación. Aplicación a imágenes y vídeo.
Procesamiento de señal forense.	Detección y estimación de cuantificación. Detección e identificación de filtrado. Detección y estimación de remuestreo. Balística de fuentes.
Procesado de señal en el dominio cifrado.	Métricas y conceptos de privacidad. Cifrado homomórfico. Circuitos ilegibles. Representación de señales y explosión de cifras. Aplicaciones.

Planificación			
	Horas en clase	Horas fuera de clase	Horas totales
Sesión magistral	14	28	42
Prácticas de laboratorio	9	42	51
Informes/memorias de prácticas	0	30	30
Pruebas de respuesta larga, de desarrollo	2	0	2

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

Metodologías	
	Descripción
Sesión magistral	El curso está estructurado en varios temas en seguridad multimedia, incluyendo criptografía, marcado de agua, forensía y procesado de señal en el dominio cifrado. Competencias: CG4, CG8, CE31
Prácticas de laboratorio	Las prácticas de laboratorio cubrirán aspectos diferentes de la ocultación de datos, marcado de agua y forensía. Esto permitirá que los estudiantes implementen y expandan considerablemente algunos de los conceptos vistos en las clases. Competences: CG4, CG8, CE31

Atención personalizada	
Metodologías	**Descripción**
Sesión magistral	Los profesores de la materia proporcionarán atención individual y personalizada a los alumnos durante lo curso, solucionando sus dudas y preguntas. Las dudas se atenderán de forma presencial (durante la propia sesión magistral, o durante el horario establecido para tutorías). El horario de tutorias se establecerá al principio del curso y se publicará en la página web de la asignatura.
Pruebas	**Descripción**

Informes/memorias de prácticas	Los profesores de la materia proporcionarán atención individual y personalizada a los alumnos durante el curso, solucionando sus dudas y preguntas. Las dudas se atenderán de forma presencial (durante las sesiones de seguimiento del trabajo, o durante el horario establecido para tutorías).

Evaluación

	Descripción	Calificación	Resultados de Formación y Aprendizaje	
Informes/memorias de prácticas	Informes de las prácticas y trabajo personal adicional que emplee las técnicas vistas en el aula. Se evaluará la calidad de los informes y la corrección de los resultados. Los informes serán individuales o colectivos, dependiendo de la unidad que ha realizado cada práctica.	70	B4 B8	C31
Pruebas de respuesta larga, de desarrollo	Examen final con cuestiones cortas sobre los contenidos del curso.	30	B4 B8	C31

Otros comentarios sobre la Evaluación

Se requiere una puntuación mínima del 30% con respecto al máximo posible en el examen final para aprobar la asignatura.

En aquellos casos en que el alumno decida no realizar las tareas de evaluación continua, la nota final se basará exclusivamente en el examen con cuestiones sobre la materia. Esto aplica también a la segunda convocatoria.

En caso de que el alumno no obtenga la puntuación mínima en el examen final escrito, la nota final se obtendrá usando la fórmula: 0.35*REP+0.15*TEST, donde REP es la nota obtenida en los informes/memorias y TEST es la nota obtenida en el examen final.

En caso de informes colectivos, se deberá explicitar la contribución de cada alumno al mismo, y la evaluación será individualizada, en función da dicha contribución. El profesor podrá requerir una entrevista para determinar las contribuciones individuales.

Una vez que el alumno entrega alguno de los entregables, está automáticamente decidiendo ser evaluado de forma continua.

Cualquier alumno decide ser evaluado de forma continua, tendrá una nota final, independientemente de si realiza el examen final o no.

Las tareas de evaluación continua no pueden repetirse después de sus correspondientes fechas de entrega, y son válidas sólo para el curso actual.

En caso de detección de plagio en alguno de los trabajos/pruebas realizadas la calificación final de la asignatura será de suspenso (0) y los profesores comunicarán a la dirección de la escuela el asunto para que tome las medidas que considere oportunas. Asimismo, los profesores comunicarán a la dirección de la escuela cualquier conducta contraria a la ética por parte de los alumnos, existiendo la posibilidad de que aquella tome las medidas oportunas.

Fuentes de información

Bibliografía Básica

Bibliografía Complementaria

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,

Recomendaciones

Asignaturas que se recomienda haber cursado previamente

Procesado Estadístico de la Señal/V05M145V01303