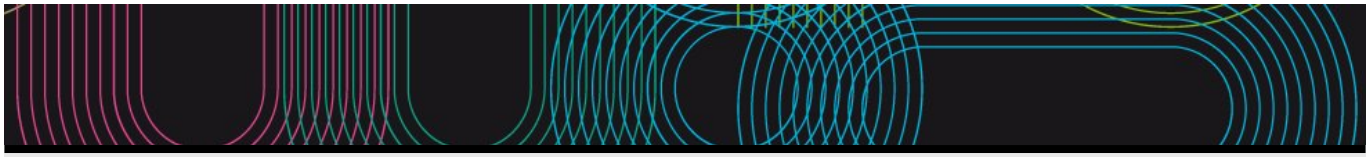

| DATOS IDENTIFICATIVOS | | | | |
|---|---|---|---|---|
| **Seguridade Multimedia** | | | | |
| Materia | Seguridade Multimedia | | | |
| Código | V05M145V01318 | | | |
| Titulación | Máster Universitario en Enxeñaría de Telecomunicación | | | |
| Descritores | Creditos ECTS | Sinale | Curso | Cuadrimestre |
| | 5 | OP | 2 | 1c |
| Lingua de impartición | Inglés | | | |
| Departamento | | | | |
| 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.<br><br>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.<br><br>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. | | | |

| Resultados de Formación e Aprendizaxe | |
|---|---|
| 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 previstos na materia | Resultados de Formación e Aprendizaxe |
|---|---|
| Comprender as capacidades e limitacións dos distintos métodos | B4<br>B8<br>C31 |
| Manexar o uso dos diferentes algoritmos nas distintas contornas de comunicacións multimedia que se poden expor actualmente. | B4<br>B8<br>C31 |

| | |
|---|---|
| Comprender material técnico de forma autónoma. | B4<br>B8<br>C31 |

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

| **Planificación** | | | |
|---|---|---|---|
| | Horas na aula | Horas fóra da aula | Horas totais |
| Lección maxistral | 14 | 28 | 42 |
| Prácticas de laboratorio | 9 | 42 | 51 |
| Informe de prácticas, prácticum e prácticas externas | 0 | 15 | 15 |
| Informe de prácticas, prácticum e prácticas externas(Repetida non usar) | 0 | 15 | 15 |
| Exame de preguntas 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 |
| Lección maxistral | O curso está estruturado en varios temas en seguridade multimedia, incluíndo criptografía, marcado de auga, forensía e procesado de sinal no dominio cifrado.<br><br>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.<br><br>Competencias: CG4, CG8, CE31 |

| **Atención personalizada** | |
|---|---|
| **Metodoloxías** | **Descrición** |
| Lección maxistral | Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse 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. Contato: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/fernando-perez-gonzalez |
| **Probas** | **Descrición** |

| | |
|---|---|
| Informe de prácticas, prácticum e prácticas externas | Os profesores da materia proporcionarán atención individual e personalizada aos alumnos durante o curso, solucionando as súas dúbidas e preguntas. As dúbidas atenderanse durante as sesións de seguimento do traballo, ou durante o horario establecido para tutorías. Contato: https://www.uvigo.gal/es/universidad/administracion-personal/pdi/fernando-perez-gonzalez |
| Informe de prácticas, prácticum e prácticas externas(Repetida non usar) | |

## Avaliación

| | Descrición | Cualificación | Resultados de Formación e Aprendizaxe | |
|---|---|---|---|---|
| Informe de prácticas, prácticum e prácticas externas | Informes das prácticas e traballo persoal adicional que empregue as técnicas vistas na aula:<br><br>Práctica 1: Marcado de auga e ocultación de datos (35%)<br><br>Avaliarase a calidade dos informes e a corrección dos resultados. Os informes serán individuais ou colectivos, dependendo da unidade que realizou cada práctica. | 35 | B4<br>B8 | C31 |
| Informe de prácticas, prácticum e prácticas externas(Repetida non usar) | Informes das prácticas e traballo persoal adicional que empregue as técnicas vistas na aula:<br><br>Práctica 2: Análisis forense (35%)<br><br>Avaliarase a calidade dos informes e a corrección dos resultados. Os informes serán individuais ou colectivos, dependendo da unidade que realizou cada práctica. | 35 | B4<br>B8 | C31 |
| Exame de preguntas de desenvolvemento | Exame final con cuestións curtas sobre os contidos do curso. | 30 | B4<br>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 oportunidade extraordinaria.
No caso de que o alumno non obteña a puntuación mínima no exame final escrito, a nota final obterase usando a fórmula: 0.35*REP+0.15*TEST, onde REP é a nota obtida nos informes/memorias e TEST é a nota obtida no exame final.
En caso de informes colectivos, deberase explicitar a contribución de cada alumno ao mesmo, e a avaliación será individualizada, en función da devandita contribución. O profesor poderá requerir unha entrevista para determinar as contribuciones individuais.
Unha vez que o alumno entrega algún dos entregables, está automaticamente decidindo ser avaliado de forma continua, sempre que houbese transcurrido máis dun mes dende o comezo das clases.
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

### Bibliografía Básica

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

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

## Recomendacións