DOCTORADO EN
CIENCIAS DE LA INGENIERÍA,
MENCIÓN EN AUTOMÁTICA
UNIVERSIDAD DE SANTIAGO DE CHILE

PROGRAMA DE ASIGNATURA

Nombre del curso	**Seguridad de Capa Física en Comunicaciones**			
Descripción del curso	**Código:** 11327	**Tipo:** Asignatura electiva	**Horas presenciales semanales TEL**: 4-0-0	**Créditos SCT-Chile**: 10
Objetivos	Objetivo general: Entregar a los(as) estudiantes los conocimientos y principios fundamentales de la seguridad de capa física siendo capaces de diferencias los ataques a nivel de canal como a nivel de hardware, conociendo las contramedidas y proponer nuevas. Objetivos específicos: • Proporcionar en forma comprensible los fundamentos de seguridad de capa física como las lineas de investigación derivadas. • Proporcionar los conceptos y diferencias de la seguridad de capa física a nivel de canal como a nivel de hardware, revisando modelos clásicos. • Analizar y evaluar nuevas métricas para determinar la existencia de secreto en un canal de comunicación. • Proporcionar y analizar contramedidas contra ataques de capa física a nivel de canal como a nivel de hardware. • Aplicar herramientas de simulación para evaluar los ataques y contramedidas. • Investigar en base al estado del arte proporcionado, técnicas utilizadas para detectar, prevenir y/o evitar ataques al canal como al hardware. • Realizar un proyecto de investigación seleccionando un tema de interés recopilando los principales artículos del tema seleccionado presentando un análisis y evaluación critica.			
Contenidos	• Introducción a la seguridad de capa física. Enfoques: Secreto en Teoría de la información. Comunicación secreta sobre canales ruidosos. Generación de la clave secreta. • Ataques de capa física. Ataques al canal de comunicación – Jammer y eavesdropper. Ataques a los dispositivos – Canal lateral y exponenziación modular. • Métricas. Capacidad de secreto. Probabilidad del error. • Contramedidas: Jammer y eavesdropper. MIMO para Seguridad de capa física. Relay, jammer y jammer cooperativo. Detección y localización jammer. • Contramedidas: Ataques de canal lateral. Algoritmos y Hardware. (RSA, ECC) • Buenas prácticas y tecnologías emergentes.			
Modalidad de evaluación	El procedimiento de evaluación se basa en evaluaciones (20%), tareas (30%) y la elaboración de un proyecto (50%) cuyo tema de interés será a elección del estudiante según línea de investigación, siempre y cuando utilice herramientas y métodos utilizados en el desarrollo del curso.			
Bibliografía	**Básica:** • Mukhopadhyay, D., y Chakraborty, R. S. (2015). Hardware security: Design, Threats and Safeguards. CRC Press Taylor & Francis Group. • Zhou, X., Song, L., y Zhang, Y. (2014). Physical Layer Security in wireless communications. CRC Press Taylor & Francis Group. • Hong, Y. W., Pang-Chang Lan, C.C., y Kuo, J. (2014). Signal processing approaches to secure physical layer communications in multi-antenna wireless systems. Springer-Verlag. • Revistas: IEEE Tutorial and Surveys, Springer, Elsevier, International workshop CHES.			
	Recomendada: • Bloch, M., y Barros, J. (2011). Physical-layer security: From information theory to security engineering. Cambridge University Press. • Koeune, F., y Standaert, F. X. (2010). Chapter 2: Introduction to Side-Channel Attacks. Secure Integrated Circuits and Systems. Springer Verlag.			