Internet cuántica y criptografía cuántica

Curso Académico: (2023 / 2024) **Fecha de revisión: 28/04/2023 15:35:51**

Departamento asignado a la asignatura: Departamento de Informática, Departamento de Ingeniería Telemática

Coordinador/a: VALERA PINTOR, FRANCISCO

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 1 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Sistemas de redes de ordenadores seguros

OBJETIVOS

Los objetivos de la asignatura son los siguientes:
- Conocer los conceptos fundamentales de la Internet cuántica y cómo se diferencia de la Internet clásica.
- Comprender la relación de la la Internet cuántica con los fundamentos de la mecánica cuántica.
- Conocer los componentes básicos de las redes cuánticas, incluyendo sistemas finales, líneas de comunicación, conmutadores y encaminadores (repetidores).
- Comprender la arquitectura de los protocolos en redes cuánticas y su implementación.
- Aprender los fundamentos y aplicaciones de la criptografía cuántica, en particular la distribución de claves.
- Conocer los conceptos básicos de la criptografía post cuántica y sus aplicaciones prácticas.
- Explorar las aplicaciones actuales y futuras de la Internet cuántica en diferentes áreas.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

- Fundamentos cuánticos de la Internet cuántica
- Redes cuánticas: sistemas finales, líneas de comunicación, conmutadores y encaminadores (repetidores)
- Arquitectura de protocolos en redes cuánticas
- Internet cuántica
- Fundamentos y aplicaciones de la criptografía cuántica: distribución de claves
- Criptografía post cuántica
- Aplicaciones de la Internet cuántica

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

Acciones formativas:
- Clase teórica
- Clases prácticas de laboratorio
- Tutorías
- Trabajo individual del estudiante
- Exámenes parciales y finales

Metodología:
- Exposiciones en clase del profesor con soporte de medios informáticos y audiovisuales, en las que se desarrollan los conceptos principales de la materia y se proporciona la bibliografía para complementar el aprendizaje de los alumnos.
- Lectura crítica de textos recomendados por el profesor de la asignatura: artículos, informes, manuales y/o artículos académicos, bien para su posterior discusión en clase, bien para ampliar y consolidar los conocimientos de la asignatura.
- Resolución de casos prácticos, problemas, etc. planteados por el profesor de manera individual o en grupo

- Exposición y discusión en clase, bajo la moderación del profesor de temas relacionados con el contenido de la materia, así como de casos prácticos
- Elaboración de trabajos e informes de manera individual o en grupo

SISTEMA DE EVALUACIÓN

Peso porcentual del Examen/Prueba Final:	60
Peso porcentual del resto de la evaluación:	40

- Trabajos individuales o en grupo realizados durante el curso, 40%
- Examen final, 60%

BIBLIOGRAFÍA BÁSICA

- Beullens, Ward ; D'Anvers, Jan-Pieter ; Hülsing, Andreas ; Lange, Tanja ; Panny, Lorenz ; Saint Guilhem, Cyprien de ; Smart, Nigel P Post-quantum cryptography: current state and quantum mitigation, Publications Office , 2021

- Federico Grasselli author Quantum cryptography : from key distribution to conference key agreement, Springer, 2021

- Kollmitzer, Christian ; Schauer, Stefan ; Rass, Stefan ; Rainer, Benjamin Quantum Random Number Generation: Theory and Practice, Springer International Publishing , 2021

- Rodney Van Meter Quantum Networking, John Wiley & Sons Ltd., 2014

BIBLIOGRAFÍA COMPLEMENTARIA

- Bernstein, Daniel J ; Hülsing, Andreas ; Lange, Tanja ; Rekleitis, Evangelos Post-quantum cryptography: integration study, Publications Office , 2022

- Roger A. Grimes Cryptography apocalypse : preparing for the day when quantum computing breaks today's crypto, Wiley , 2020

RECURSOS ELECTRÓNICOS BÁSICOS

- Chonggang Wang, Akbar Rahman, Ruidong Li, Melchior Aelmans, Kaushik Chakraborty . Application Scenarios for the Quantum Internet: https://datatracker.ietf.org/doc/draft-irtf-qirg-quantum-internet-use-cases/

- Wojciech Kozlowski, Stephanie Wehner, Rodney Van Meter, Bruno Rijsman, Angela Sara Cacciapuoti, Marcello Caleffi, Shota Nagayama . Architectural Principles for a Quantum Internet: https://datatracker.ietf.org/doc/rfc9340/