PROPUESTA MODULO DE TALLER (*para aprobación por la Comisión de Carrera*)

Nombre Actividad Específica	***Criptografía basada en Códigos y Reticulados***
Proponente	*IMERL*
Responsable	*Claudio Qureshi*
Responsable en INCO o FING	*Claudio Qureshi*
Objetivo	*Familiarización con los fundamentos de criptografía clásica y pos-cuántica. Comprensión básica de la teoría de códigos correctores de errores, incluyendo algunas construcciones y relación con criptografía. Introducción a los fundamentos matemáticos de los reticulados, incluyendo nociones básicas de geometría de números. Análisis de problemas computacionales utilizados en criptografía pos-cuántica, como el problema de la decodificación y el problema del vector más corto (SVP)*
Descripción	*Se realizaran exposiciones de 2 horas semanales por parte de los participantes bajo la orientación del responsable quien le brindará todo el material relativo a la preparación de la exposición y contarán con horario de consulta para evacuar dudas. El estudiante deberá contar con al menos el 75% de asistencia. Los tópicos de las exposiciones se detallan a continuación (Obs. cada tópico puede llevar más de una exposición):* • *Criptografía clásica de clave pública, problema del logaritmo discreto y de factorización, método Diffie-Hellman, criptosistemas RSA y ElGammal. Reducción del problema de factorización al problema de hallar el período de una función y relación con computación cuántica.* • *Computación cuántica: qubits, puertas lógicas y cuánticas, circuitos cuánticos, algoritmos cuánticos.* • *Cuerpos finitos, códigos lineales y sus parámetros. Familia de códigos: Hamming y Reed-Solomon.* • *Geometría algebraica y códigos de Goppa. Decodificación por síndrome.* • *Esquema de McElliese y variante de Niederreiter.* • *Reticulados y geometría de números, Teorema de Minkowski.* • *SVP, CVP, Algoritmo LLL y reducción de bases.* • *Criptosistemas NTRU, Kyber y Dilithium*
Aporte a / tareas concretas del/la estudiante	*Se espera que el estudiante se familiarize con conceptos de criptografía pos-cuántica principalmente con aquellos criptosistemas basados en códigos y reticulados. Cada estudiante deberá preparar dos exposiciones y participar activamente de todas las clases.*
Carga horaria total	*60 horas*
Créditos (no más de 10)	*4*
Fecha inicio	*26/03/2025*
Duración/Plazo	*13 semanas*

Conocimientos requeridos	*Aritmética y teoría de grupos (al nivel del curso de Matemática Discreta 2)*
Cupo de estudiantes	*No hay cupos máximos*
Forma de Selección	*No corresponde*
Método de Evaluación	*Participación activa durante todo el período y preparación de dos exposiciones orales.*

Firma docente responsable
inco – fing

aprobado Comisión Carrera fecha: