FORMULARIO 2025
Seminario de Posgrado

1. Título:
Criptografía basada en Códigos y Reticulados

---

2. Profesor:
Claudio Qureshi

3. Responsable:
(en caso de no ser el Profesor un investigador del PEDECIBA)

---

4. Marque la disciplina más cercana al curso:

- Álgebra
- Análisis
- Análisis numérico
- Ecuaciones diferenciales; EDP
- Estadística
- Fundamentos
- Geometría
- Geometría algebraica
- Matemática Aplicada (X)
- Probabilidad
- Sistemas Dinámicos
- Teoría de Números
- Otros: Matemática Discreta

---

5. Fecha de inicio: 17-03-2025

6. Fecha de finalización estimada: 04-07-2025

---

7. Horas de reunión semanal: 2 horas

---

8. Conocimientos previos recomendados: Álgebra lineal, Matemática Discreta, Probabilidad, Teoría de números

---

9. Método de aprobación del seminario: 2 exposiciones orales (eventualmente en duplas)
(cantidad de exposiciones por estudiante)

10. Programa del Seminario:

1. Introducción a la criptografía clásica y pos-cuántica: Conceptos básicos: confidencialidad, integridad y autenticación. Método de acuerdo de clave Diffie-Helman. Criptografía de clave pública RSA y ElGamal. Computación cuántica: algoritmos de Shor y Grover.
2. Teoría básica de códigos correctores de errores. Cuerpos finitos. Códigos lineales, parámetros fundamentales (longitud, dimensión y distancia mínima). Matriz generadora, matriz de control de paridad y relación con la distancia mínima de un código. Códigos de Hamming, códigos de Reed-Solomon y códigos de Goppa (algabraico-geométricos). Decodificación mediante síndrome.
3. Criptografía basada en códigos: Uso de códigos de Goppa en el criptosistema de McEliece, descripción y análisis de seguridad. Esquema de Niederreiter: relación con la decodificación mediante síndrome. Ataques conocidos y variantes modernas.
4. Introducción a los reticulados y la geometría de números: Reticulados, propiedades básicas, teorema de Minkowski. Problema del vector más corto y del vector más cercano (SVP y CVP). Nociones de reducción de bases: algoritmo LLL y sus aplicaciones.
5. Criptografía basada en reticulados: Estudio de criptosistemas NTRU, Kyber y Dilithium.

11. Bibliografía:

1. Hoffstein, J., Pipher, J., & Silverman, J. H. (2008). An Introduction to Mathematical Cryptography. Springer.
2. Bernstein, D. J., Buchmann, J., & Dahmen, E. (Eds.). (2009). Post-Quantum Cryptography. Springer.
3. Lidl, R., & Niederreiter, H. (1997). Introduction to Finite Fields and Their Applications. Cambridge University Press.
4. Micciancio, D., & Goldwasser, S. (2002). Complexity of Lattice Problems: A Cryptographic Perspective. Springer.
5. Galbraith, S. D. (2012). Mathematics of Public Key Cryptography. Cambridge University Press.

Otras referencias:

•Huffman, W. Cary, and Vera Pless. Fundamentals of error-correcting codes. Cambridge university press, 2010.
•F. J. MacWilliams, N. J. A. Sloane. The Theory of Error-Correcting Codes. Elsevier Science Publishers 2: 39-47, 1977.
•Henk van Tilborg, Introduction to Cryptology. Kluwer Academic Publishers, 1987.
•D. J. Bernstein, T. Lange, C. Peters. Attacking and defending the McEliece cryptosystem. In Post-Quantum Cryptography: Second International Workshop, PQCrypto 2008 Cincinnati, OH, USA, October 17-19, 2008 Proceedings 2 (pp. 31-46). Springer Berlin Heidelberg. 2008.
•H. Niederreiter. Error-correcting codes and cryptography. Public-Key Cryptosystem and Computational Number Theory, Alster, K., Urabanowicz, J. and Williams, HC (Eds.), Walter de Gruyter, 209-219. 2001.
•Otras referencias: https://pqcrypto.org/code.html