Nombre de la Asignatura	Criptografía: aspectos teóricos y prácticos
Créditos	12 Créditos
Objetivo de la Asignatura	El objetivo de la asignatura es que los estudiantes conozcan la manera que la teoría de números se aplica a la criptografía. Aprenderán los fundamentos matemáticos de la criptografía, las principales primitivas criptográficas, varios protocolos, tanto implementarlos como algunas prácticas de como hacerlos vulnerables.
Metodología de enseñanza	Se dictarán 3 horas semanales de teórico y 2 horas semanales de práctico. Asignaciones en la Facultad de Ingeniería: **Martes** de 11:30 a 13 horas el salón 106 (teórico); **Jueves** de 11:30 a 13 horas el salón 106 (teórico) y **Viernes** de 11:30 a 13:30 horas el salón 105 (práctico).
Temario	1. **Introducción:** ¿Qué es la criptografía y para que se usa?; ¿Cómo se integra con otros aspectos de seguridad informática?; ¿Qué tipo de problemas se quiere resolver con la criptografía?; Cifrados básicos; Teoría elemental de números; Criptografía antes la época de computadoras; Cifrados simétricos y asimétricos. 2. **Logaritmo discreto (DLP) y Diffie-Hellman (DH):** La invención de la criptografía de clave pública; El DLP; DH; ElGamal; Repaso de teoría de grupos; ¿Qué difícil es el DLP?; Un algoritmo de colisión; El teorema chino de los restos; Pohlig-Hellman; Anillos, cocientes, polinomios y cuerpos finitos. 3. **Factorización y RSA:** Fórmula de Euler, RSA, Aspectos de la implementación y seguridad; Tests de primalidad; Algoritmo p-1 de Pollard; Otros métodos de factorización. 4. **Combinatoria, Probabilidad y Teoría de Información:** Repaso de como contar; El cifrado de Vigenère; Repaso de probabilidad; Método de Pollard; Elementos de la teoría de información; Elementos de la teoría de complejidad: P vs NP. 5. **Curvas elípticas (EC) y criptografía:** EC, en particular sobre cuerpos finitos; Criptografía con curvas elípticas (ECC); La evolución de criptografía de clave pública; Factorizando con el algoritmo de Lenstra; Pairings. 6. **Retículos y criptografía:** Cifrados de tipo knapsack; Repaso de espacios vectoriales; Retículos; Vectores cortos en retículos; El algoritmo de Babai; Problemas de retículos difíciles y aptos para la criptografía; Los sistemas GGH y NTRU; El algoritmo LLL con aplicaciones criptográficas. 7. **Firmas digitales:** ¿Qué son?; Firmas usando RSA, ElGamal, GGH y NTRU. 8. **Otros temas:** Funciones hash; Números aleatorios y pseudo-aleatorios; Pruebas de Zero-Knowledge.

Bibliografía	1. “An Introduction to Mathematical Cryptography” por J. Hoffstein, J. Pipher y J. Silverman 2. “Cryptography: Theory and Practice, Third Edition” por D. Stinson 3. “An Introduction to Number Theory with Cryptography” por J. Kraft y L. Washington 4. “Applied Cryptography” por B. Schneier 5. “Cryptography: An Introduction” por N. Smart http://www.cs.umd.edu/%7Ewaa/414-F11/IntroToCrypto.pdf
Conocimientos previos recomendados	Conocimientos de matemática discreta y conocimientos básicos de programación.

Anexo:
Cronograma tentativo (15 semanas).

- Semanas 1 y 2: Introducción
- Semanas 3 a 5: DLP y DH
- Semanas 6 a 8: RSA y factorización
- Semana 9 y 10 : EC y criptografía
- Semana 11 a 13: Retículos y criptografía
- Semana 14: Firmas digitales
- Semana 15: Otros temas

Modalidad del curso y procedimiento de evaluación.

Cada semana escucharán 3 horas de exposición teórica sobre los temas del curso y trabajaran junto con el ayudante durante 2 horas de práctico en listas de ejercicios y

laboratorios.

Procedimiento de evaluación

- Seis listas de ejercicios (30 %)
- Cinco laboratorios (30 %)
- Examen final (40 %)

Para la aprobación final del curso se requiere un mínimo de 60% de los puntos en cada parte y un mínimo de 60% en el total.

Materia.

Licenciatura en Computación: Matemática
Ingeniería en Computación: Matemática

Previaturas.

Examen de Matemática Discreta 2
Examen de Programación 3

Cupo

No hay cupo para este curso.

Esta asignatura no adhiere a resolución del consejo sobre condición de libre