PLAN DE ESTUDIOS (PE): Licenciatura en Matemáticas

ÁREA: Álgebra

ASIGNATURA: Criptografía

CÓDIGO:

CRÉDITOS: 6

FECHA: Julio 2017

1. DATOS GENERALES

Nivel Educativo:	Licenciatura
Nombre del Plan de Estudios:	Licenciatura en Matemáticas
Modalidad Académica:	Presencial
Nombre de la Asignatura:	Criptografía
Ubicación:	Nivel formativo
Correlación:	
Asignaturas Precedentes:	Anillos y Campos, Teoría de Números
Asignaturas Consecuentes:	

2. CARGA HORARIA DEL ESTUDIANTE

Concepto	Horas por semana		Total de horas por periodo	Total de créditos por periodo
	Teoría	Práctica		
Horas teoría y práctica (16 horas = 1 crédito)	**3**	**2**	**100**	**6**

3. REVISIONES Y ACTUALIZACIONES

Autores:	David Villa Hernández, César Cejudo Castilla, Iván Fernando Vilchis Montalvo, Carlos Alberto López Andrade
Fecha de diseño:	Julio 2017
Fecha de la última actualización:	No aplica
Fecha de aprobación por parte de la academia de área, departamento u otro.	06/07/2017
Revisores:	No aplica
Sinopsis de la revisión y/o actualización:	No aplica

4. PERFIL DESEABLE DEL PROFESOR (A) PARA IMPARTIR LA ASIGNATURA:

Disciplina profesional:	Matemático
Nivel académico:	Licenciatura
Experiencia docente:	0 años
Experiencia profesional:	0 años

5. PROPÓSITO: Introducir al alumno en el tema de la seguridad de la información digital a través del estudio de los criptosistemas de llave privada y pública desde un enfoque algebraico.

6. COMPETENCIAS PROFESIONALES:

1. Conocer los conceptos y métodos básicos de la criptografía
2. Implementar en la computadora algoritmos de cifrado clásicos y modernos, de llave privada y llave pública.

7. CONTENIDOS TEMÁTICOS

Unidad de Aprendizaje	Contenido Temático	Referencias

Unidad de Aprendizaje	Contenido Temático	Referencias
1. Conceptos Básicos de Criptografía	1.1. Seguridad de la información y criptografía 1.2. Terminología y conceptos básicos 1.3. Funciones 1-1, funciones unidireccionales (one-way) y funciones trampa unidireccional (trapdoor one-way) 1.4. Teoría de la complejidad. 1.5. Criptografía simétrica (Criptosistema de llave privada) 1.6. Firma digital 1.7. Autenticación e identificación 1.8. Criptografía asimétrica (Criptosistema de llave pública)	1. Menezes A. J., van Oorschot P. C. and Vanstone S. A, Handbook of Applied Cryptography, First Edition, CRC Pres Taylor & Francis Group,1997 2. McAndrew A., Introduction to Cryptography with Open-Source Software, First Edition, CRC Press Taylor & Francis Group, 2011 3. Rothe J., Complexity Theory and Cryptology: An Introduction to Cryptocomplexity, First Edition, Springer-Verlag, 2005} 4. von zur Gathen J., CryptoSchool, First Edition, Springer-Verlag, 2015
2. Criptosistemas Clásicos	2.1 Cifrado de Julio César 2.2 Cifrados de traslación 2.3 Cifrados de transposición 2.4 Criptoanálisis de los cifrados de traslación y transposición 2.5 Cifrado de Vigenère 2.6 Criptoanálisis del cifrado de Vigenère 2.7 Cifrados de permutación 2.8 Cifrados matriciales 2.9 Criptoanálisis de los cifrados de permutación y de los cifrados matriciales.	1. McAndrew A., Introduction to Cryptography with Open-Source Software, First Edition, CRC Press Taylor & Francis Group, 2011 2. Stinson D. R., Cryptography: Theory and Practice, Third Edition, Chapman & Hall/CRC Taylor & Francis Group, 2006 3. Menezes A. J., van Oorschot P. C. and Vanstone S. A, Handbook of Applied Cryptography, First

Unidad de Aprendizaje	Contenido Temático	Referencias
		Edition, CRC Pres Taylor & Francis Group,1997 4. van Tilborg H. C. A., Fundamentals of Cryptology, First Edition, Kluwer Academic Publishers, 2002 5. Buchmann J., Introduction to Cryptography, Second Edition, Springer, 2004 6. von zur Gathen J., CryptoSchool, First Edition, Springer-Verlag, 2015
3. Breve Reseña de los Criptosistemas de Llave Secreta: DES y AES	3.1 DES: Descripción y análisis. 3.2 AES: Descripción y análisis	1. McAndrew A., Introduction to Cryptography with Open-Source Software, First Edition, CRC Press Taylor & Francis Group, 2011 2. Stinson D. R., Cryptography: Theory and Practice, Third Edition, Chapman & Hall/CRC Taylor & Francis Group, 2006 3. Buchmann J., Introduction to Cryptography, Second Edition, Springer, 2004 4. von zur Gathen J., CryptoSchool, First Edition, Springer-Verlag, 2015 5. Menezes A. J., van Oorschot P. C. and Vanstone S. A, Handbook of Applied Cryptography, First Edition, CRC Pres Taylor & Francis Group,1997

Unidad de Aprendizaje	Contenido Temático	Referencias
		6. Delfs H., and Knebl H., Introduction to Cryptography: Principles and Applications, Third Edition, Springer-Verlag, 2015 7. van Tilborg H. C. A., Fundamentals of Cryptology, First Edition, Kluwer Academic Publishers, 2002
4. Los Criptosistemas de Llave Pública: RSA, ElGamal y McEliece	4.1 Acercamiento a la generación de números primos grandes 4.2 Distribución de números primos 4.3 Pruebas de primalidad probabilística 4.4 Principios básicos de la criptografía de llave pública 4.5 El criptosistema de llave pública RSA: descripción, seguridad e implementación 4.6 El criptosistema de llave pública ElGamal: el encriptado básico de ELGamal y el encriptado generalizado de ElGamal 4.7 El criptosistema de llave pública de McEliece	1. Menezes A. J., van Oorschot P. C. and Vanstone S. A, Handbook of Applied Cryptography, First Edition, CRC Pres Taylor & Francis Group,1997 2. McAndrew A., Introduction to Cryptography with Open-Source Software, First Edition, CRC Press Taylor & Francis Group, 2011 3. Stinson D. R., Cryptography: Theory and Practice, Third Edition, Chapman & Hall/CRC Press, 2006 4. Hoffstein J., Pipher J., and Silverman J. H., An Introduction to Mathematical Cryptography, First Edition, Springer, 2008 5. Delfs H., and Knebl H., Introduction to Cryptography: Principles and Applications, Third Edition, Springer-Verlag, 2015

Unidad de Aprendizaje	Contenido Temático	Referencias
		6. von zur Gathen J., CryptoSchool, First Edition, Springer-Verlag, 2015 7. 8. Buchmann J., Introduction to Cryptography, Second Edition, Springer, 2004 9. Rothe J., Complexity Theory and Cryptology: An Introduction to Cryptocomplexity, First Edition, Springer-Verlag, 2005 10. van Tilborg H. C. A., Fundamentals of Cryptology, First Edition, Kluwer Academic Publishers, 2002
5. Introducción a la Criptografía de Curvas Elípticas	5.1. Introducción a las curvas elípticas sobre campos finitos 5.2. El método de factorización en curvas elípticas 5.3. El problema del logaritmo discreto en curvas elípticas	1. Ling S., Wang H., and Xing C., Algebraic Curves in Cryptography, First Edition, CRC Press Tayloy & Francis Group, 2013 2. Hankerson D., Menezes A., and Vanstone S., Guide to Elliptic Curve Cryptography, First Edition, Springer-Verlag, 2004 3. Washington L. C., Elliptic Curves: Number Theory and Cryptography, Second Edition, Chapman & Hall/CRC Taylor & Francis Group, 2004 4. McAndrew A., Introduction to Cryptography with Open-

Unidad de Aprendizaje	Contenido Temático	Referencias
		Source Software, First Edition, CRC Press Taylor & Francis Group, 2011 5. Hoffstein J., Pipher J., and Silverman J. H., An Introduction to Mathematical Cryptography, First Edition, Springer, 2008 6. Delfs H., and Knebl H., Introduction to Cryptography: Principles and Applications, Third Edition, Springer-Verlag, 2015 7. von zur Gathen J., CryptoSchool, First Edition, Springer-Verlag, 2015 8. Stinson D. R., Cryptography: Theory and Practice, Third Edition, Chapman & Hall/CRC Press, 2006 9. van Tilborg H. C. A., Fundamentals of Cryptology, First Edition, Kluwer Academic Publishers, 2002

8. ESTRATEGIAS, TÉCNICAS Y RECURSOS DIDÁCTICOS

Estrategias y técnicas didácticas	Recursos didácticos

Estrategias de aprendizaje: El estudiante trabajará en forma individual, por equipo y colectiva en la comprensión de conceptos y la resolución de problemas. Asistirá a asesorías para resolver dudas sobre la teoría o sobre la solución de problemas. Estrategias de enseñanza: El profesor explicará la teoría y presentará ejemplos. Aportará ideas sobre los métodos para resolver los problemas. Motivará a los estudiantes para trabajar de manera individual, colectiva y en equipo. Generará un ambiente de confianza y de compromiso con el grupo. Interaccionará con los estudiantes para conocer sus problemas en el aprendizaje. Ofrecerá asesorías. Se tendrán clases de exposición de la teoría. Trabajo en equipo y colectivo para la solución de problemas. Se ofrecerán asesorías individuales en horario propuesto por el profesor.	• Libro de texto • Bibliografía complementaria. • Listas de ejercicios. • Uso de software.

9. EJES TRANSVERSALES

Eje (s) transversales	Contribución de la asignatura
Formación Humana y Social	La matemática como actividad creativa nos conduce a un mejor conocimiento de la naturaleza del hombre.
Desarrollo de Habilidades en el uso de las Tecnologías de la Información y la Comunicación	Diversos programas computacionales están fundamentados por el profundo conocimiento del álgebra lineal, la cercanía a estas estructuras matemáticas nos introduce a problemas tecnológicos e informáticos.
Desarrollo de Habilidades del Pensamiento Complejo	La matemática como una forma abstracta de pensar al mundo, implica un desarrollo complejo del pensamiento.
Lengua Extranjera	Diversa bibliografía del tema está en inglés.
Innovación y Talento Universitario	La matemática siempre es innovación, en cualquiera de sus estados.
Educación para la Investigación	Cotidianamente la actividad matemática se realiza dentro de un formato de investigación.

10. CRITERIOS DE EVALUACIÓN

Criterios	Porcentaje
▪ Exámenes	50%
▪ Exposiciones	50%
Total	100%

11. REQUISITOS DE ACREDITACIÓN

Estar inscrito como alumno en la Unidad Académica en la BUAP
Asistir como mínimo al 80% de las sesiones para tener derecho a exentar por evaluación continua y/o presentar el examen final en ordinario o extraordinario
Asistir como mínimo al 70% de las sesiones para tener derecho al examen extraordinario
Cumplir con las actividades académicas y cargas de estudio asignadas que señale el PE