UNIDAD: **IZTAPALAPA**	DIVISIÓN **CIENCIAS BÁSICAS E INGENIERÍA**	
NIVEL: **LICENCIATURA**	EN **MATEMÁTICAS**	
CLAVE: **2131131**	UNIDAD DE ENSEÑANZA - APRENDIZAJE: **CRIPTOGRAFÍA DE CLAVE PÚBLICA**	TRIM: **VIII**
HORAS TEORÍA:**3**		CRÉDITOS: **9**
HORAS PRÁCTICA: **3**	SERIACIÓN **2131108 Y 72 CRÉDITOS DE FD**	OPT/OBL: **OPT.**

OBJETIVO(S)

GENERALES

Al finalizar el curso el alumno será capaz de:

- Comprender la importancia de cifrar mensajes.
- Comprender los modelos criptográficos clásicos.
- Aplicar algunos de los modelos criptográficos que se utilizan actualmente.
- Analizar las normas internacionales sobre criptografía.
- Expresar en forma oral y escrita los procedimientos y algoritmos utilizados así como sus conclusiones.

CONTENIDO SINTÉTICO

1. **Introducción** (3 semanas)
   - 1.1. Motivación del uso de la Criptografía. Aplicaciones actuales de la Criptografía.
   - 1.2. Sustitución simple y poli-alfabética. (Cifrados tipo Julio César, Vigenere, etc.)
   - 1.3. Algunas técnicas de cripto-análisis.
   - 1.4. Modelos de cifrado de Playfair y de Hill.
   - 1.5. Secreto perfecto.
2. **Cifrados de llave privada** (3 semanas)
   - 2.1. El criptosistema DES.
   - 2.2. El criptosistema AES.
   - 2.3. Aplicaciones.
3. **Cifrados en flujo** (3 semanas)
   - 3.1. Descripción de los cifrados en flujo.
   - 3.2. Generadores de números pseudoaleatorios.
   - 3.3. Registros lineales con retroalimentación.
4. **Normas de seguridad para redes de comunicación.** (2 semanas)

MODALIDADES DE CONDUCCIÓN DEL PROCESO DE ENSEÑANZA-APRENDIZAJE

Es recomendable que al inicio del curso se asigne un trabajo sobre las definiciones y propiedades principales de los campos con *p* elementos, donde *p* es un número primo. Este tema debe ser conocidos por los alumnos y se utilizarán frecuentemente a lo largo del curso.

Los alumnos deberán asistir al laboratorio de Códigos y Criptografía por los menos en dos ocasiones al mes, y a todas las sesiones del seminario permanente de Códigos y Criptografía.

Se recomienda que el alumno resuelva algunos ejercicios con la ayuda de un programa de cómputo, por ejemplo Mathematica, Maple o GAP.

NOMBRE DEL PLAN LICENCIATURA EN MATEMÁTICAS	2/2
CLAVE **2131131**	**UNIDAD DE DE ENSEÑANZA-APRENDIZAJE** **CRIPTOGRAFÍA DE CLAVE PÚBLICA**

Se utilizará, en la medida de lo posible, material de apoyo basado en las Tecnologías de la información y la comunicación.
El profesor promoverá que durante el transcurso de las horas teóricas y prácticas los alumnos expresen sus ideas y las expongan ante sus compañeros de manera que desarrollen su capacidad de comunicación oral.
El profesor fomentará que los alumnos realicen trabajos escritos en los que desarrollen su capacidad para comunicar sus ideas en forma escrita.
El profesor impulsará la elaboración de carteles o presentaciones en las que los alumnos comuniquen los conceptos aprendidos.
El profesor tomará especial cuidado en que los alumnos identifiquen y comprendan los argumentos correctos y erróneos tanto en sus participaciones en las clases como a través de sus trabajos escritos.

MODALIDADES DE EVALUACIÓN

GLOBAL

El profesor llevará a cabo al menos dos evaluaciones periódicas y, en su caso, una terminal. En la integración de la calificación se incorporarán aspectos como el desempeño en la solución de listas de ejercicios, la participación en clase y talleres, y la elaboración y presentación de proyectos. Los factores de ponderación serán a juicio del profesor.
En el proceso de evaluación el alumno deberá mostrar su capacidad de comprender y aplicar los conceptos desarrollados en el curso.

RECUPERACIÓN

A juicio del profesor, consistirá en una evaluación que incluya todos los contenidos teóricos y prácticos de la UEA o solo aquellos que no fueron cumplidos durante el trimestre.

BIBLIOGRAFÍA NECESARIA O RECOMENDABLE

1. Cortés Dávalos, A., et. al. *Elementos de Criptografía Clásica*. Serie Matemática Aplicada y Enseñanza. SMM, 2005, ISBN 968-5733-05-8.
2. Delfs, H., Knebl, H., *Introduction to Cryptography: Principles and Applications*. Springer, 2002.
3. Koblitz, N., *A Course in Number Theory and Cryptography*. Springer-Verlag, 1994.
4. Menezes, A. (Editor), *Applications of finite fields*., Kluwer Academic Press, 1993.
5. Menezes, A., van Oosrcot, P. C., Vanstone, S. A., *Handbook of Applied Cryptography*. CRC Press, 1996.
6. Paar, C., Pelzl, J., *Understanding Cryptography*, Spinger-Verlag, 2010.
7. Robling, D. E., *Cryptography and Data Security*, Addison-Wesley, 1983.
8. Schneier, B., *Applied Cryptography*, John Willey & Sons, 1996.
9. Stinson, D. R., *Cryptography: Theory and Practice*, CRC Press, 2006.