



1	2
---	---

UNIDAD IZTAPALAPA	DIVISIÓN C.B.I.
-----------------------------	---------------------------

POSGRADO EN MATEMÁTICAS	TRIMESTRE I al IX
--------------------------------	-----------------------------

CLAVE 2138027	UNIDAD DE ENSEÑANZA-APRENDIZAJE TECNICAS CRIPTOGRAFICAS OBL. () OPT. (X)	CREDITOS 9
-------------------------	--	----------------------

HORAS TEORIA 4.5	HORAS PRACTICA 0	SERIACIÓN Autorización
-------------------------	-------------------------	----------------------------------

OBJETIVO(S):

1. Familiarisar al alumno con los conceptos básicos de Criptografía.
2. Reconocer los alcances y limitaciones de algunos sistemas criptográficos.
3. Usar herramientas matemáticas en sistemas criptográficos.
4. Ser capaz de justificar el funcionamiento y seguridad de algunos de los principales sistemas de cifrado.

CONTENIDO SINTETICO

1. **Introducción, motivación e historia de la Criptografía. Tipos de cifrado.**
2. **Ejemplos de cifrados clásicos:** Substitución monoalfabética y polialfabética. Transposición. El grupos simétrico en Criptografía.
3. **Cifrados de llave privada.** DES, IDEA y AES.
4. **Cifrados de llave pública.** RSA y ElGamal. Análisis de la seguridad.
5. **Intercambio de Llaves de Diffie-Hellman. El Problema del Logaritmo Discreto.**
6. **Algunos servicios que proporciona la Criptografía.**



MODALIDADES DE CONDUCCION DEL PROCESO DE ENSEÑANZA-APRENDIZAJE

El profesor impartirá la mayoría de las lecciones y destinará algunas sesiones a la resolución de ejercicios. El alumno expondrá algunos de los temas del curso. Se utilizará algún manipulador algebraico para analizar sistemas criptográficos descritos en clase. Se motivará al alumno a utilizar algún programa de cómputo en la solución de algunos ejercicios. La asistencia y participación en el Seminario permanente de Criptografía será parte de las actividades de la UEA. El alumno podrá hacer uso del Laboratorio de Códigos y Criptografía.

MODALIDADES DE EVALUACIÓN

Se sugiere que la evaluación se realice mediante presentaciones, discusiones y series de problemas que los alumnos deberán entregar periódicamente.

BIBLIOGRAFÍA:

1. Cid, C. et al. *Algebraic Aspects of the Advanced Encryption Standard*. Springer, 2006.
2. Daemen, J. & Rijmen, V. *The Design of Rijndael*. Information Security and Cryptography, Text and Monographs, Springer Verlag, 2002.
3. Hankerson, D. Menezes, A. Vanstoen, S. *Guide to Elliptic Curve Cryptography*. Springer Professional Computing, Springer, 2004.
4. Kaufman, Ch. et al. *Network Security: Private communications in a public world*. Prentice Hall PTR, 2nd ed., 2002.
5. Khan, D. *The Codebreakers*. Scribner, 1996.
6. Koblitz, N.I. *A Course in Number Theory and Cryptography*. Springer Verlag, 1994.
7. Lidl, R., Niederreiter, H. *Finite Fields*. Addison-Wesley, 1983.
8. Menezes, A.J. et al., *Handbook of Applied Cryptography*. CRC Press, 1997, (<http://www.carc.math.uwaterloo.ca/hac/>).
9. Mollin, R. A. *RSA and Public-Key Cryptography*. Chapman & Hall, 2002.
10. Nathason, M.B. *Elementary Methods in Number Theory*. GTM, Springer Verlag, 2000.
11. Robling, D.E. *Cryptography and Data Security*. Addison Wesley, 1987.
12. Schneier, B. *Applied Cryptography*. John Wiley & Sons, 1997.
13. Shoup, V. *A computational Introduction to Number Theory and Algebra*. Cambridge University Press, 2005.
14. Singh, S. *The code book*. Doubleday, 1999.
15. Stinson, D. R. *Cryptography: Theory and Practice*. Chapman & Hall/CRC, 3rd ed., 2006.

SELLO





Casa abierta al tiempo

UNIVERSIDAD AUTONOMA METROPOLITANA

