Casa abierta al tiempo
UNIVERSIDAD AUTONOMA METROPOLITANA

PROGRAMA DE ESTUDIOS

UNIDAD **IZTAPALAPA**	DIVISION **CIENCIAS BASICAS E INGENIERIA**	1 / 3
NOMBRE DEL PLAN **MAESTRIA EN CIENCIAS (MATEMATICAS)**		

CLAVE	UNIDAD DE ENSEÑANZA-APRENDIZAJE	CREDITOS 9
213806	**FUNDAMENTOS MATEMATICOS DE CODIGOS Y CRIPTOGRAFIA**	TIPO **OPT.**
H.TEOR. **4.5**		TRIM. **I AL II**
H.PRAC. **0.0**	SERIACION **AUTORIZACION**	

OBJETIVO(S):

Que el alumno conozca y aplique los conceptos y métodos básicos de las estructuras algebraicas básicas que se aplican en criptografía y teoría de códigos. El alumno será capaz de aplicar sus conocimientos de programación estructurada en la solución de problemas de aplicación.

CONTENIDO SINTETICO:

1. CONCEPTOS DE ÁLGEBRA.

Grupos, anillos, campos, anillos de polinomios.

2. TEORÍA DE NÚMEROS.

Aritmética modular. Teoremas de Fermat y Euler. Algoritmos. Teorema Chino del residuo. Residuos Cuadráticos. Símbolos de Legendre y Jacobi.

3. CAMPOS FINITOS Y ANILLO DE POLINOMIOS.

Conceptos básicos y ejemplos de campos finitos. Construcción de campos finitos. Ejemplos.
Propiedades básicas de campos finitos. Anillo de polinomios y el algoritmo de Euclides. Automorfismo de Frobenious, Traza.

UNIVERSIDAD AUTONOMA METROPOLITANA
CASA ABIERTA AL TIEMPO

APROBADO POR EL COLEGIO ACADEMICO
EN SU SESION NUM. 255
EL SECRETARIO DEL COLEGIO

CLAVE **213806** | **FUNDAMENTOS MATEMATICOS DE CODIGOS Y CRIPTOGRAFIA**

4. PROBABILIDAD.

Definiciones básicas. Variables aleatorias. Distribución binomial. Ataque del "cumpleaños".

5. TEORÍA DE LA INFORMACIÓN.

Entropía. Secreto perfecto.

6. COMPLEJIDAD COMPUTACIONAL.

Objetivos. Notación "O". Longitud de números. Clases de complejidad.

7. APLICACIONES.

Uso de sistemas algebraicos computacionales como Maple®, Mahtematica®, Macaulay® . Programación para realizar aritmética sobre diversas estructuras algebraicas.

MODALIDADES DE CONDUCCION DEL PROCESO ENSEÑANZA-APRENDIZAJE:

Los temas básicos del curso serán expuestos por el profesor.

MODALIDADES DE EVALUACION:

Al menos dos evaluaciones periódicas y/o una evaluación terminal, 80%.
Ejercicios en diversos ambientes computacionales, 20%.

BIBLIOGRAFIA NECESARIA O RECOMENDABLE:

1. Hibbard A. C. and Levasseur, K.M., Exploring Abstract Algebra with Mathematica. Springer , 1999.

2. Koblitz N. I., Algebraic Aspects of Cryptography. Algorithms and

Computation in Mathematics, vol. 3, Springer, 1998.

3. Koblitz N. I., A Course in Number Theory and Cryptography (Graduate Texts in Mathematics, No 114), Springer Verlag, 2nd ed., 1994.

4. Lidl R. and Niederreiter, H., Finite Fields. Addison-Wesley, 1983.

5. MacWilliams F. J. and Sloane, N.J.A., The Theory of Error-Correcting Codes. North Holland, 1977.

6. Mao W., Modern Cryptography: Theory and Practice, Prentice Hall PTR; 1st ed., 2003.

McEliece R. J., Finite Fields for Computer Scientist and Engineers. The Kluwer International Series in Engineering and Computer Sciences, Boston, 1982.

8. Menezes A. J. et al., Applications of Finite Fields. Kluwer Academic Publishers, 1993.

9. Menezes A. J. et al., Handbook of Applied Cryptography. CRC Press, 1997, (http://www.carc.math.uwaterloo.ca/hac/).

10. Menezes et al., Applications of Finite Fields. Kluwer Academic Publishers, 1993.

11. Roman S., Field Theory, Springer Verlag, 1995.

12. Shparlinski I., Computational and Algorithmic Problems in Finite Fields. Kluwer Academic Publishers, 1992.

13. Stinson D. R., Cryptography: Theory and Practice. CRC Press, 1995.

14. Wagon S., Mathematica in Action. 2nd ed., Springer, 1999.

15. Washington L. C., Elliptic Curves: Number Theory and Cryptography (Discrete Mathematics and Its Applications), Chapman & Hall, 2003.

UNIVERSIDAD AUTONOMA METROPOLITANA

CASA ABIERTA AL TIEMPO

APROBADO POR EL COLEGIO ACADEMICO

EN SU SESION NUM. 355

EL SECRETARIO DEL COLEGIO