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
213811	**CRIPTOGRAFIA II**	TIPO **OPT.**
H.TEOR. 4.5		TRIM. **II AL VI**
H.PRAC. 0.0	SERIACION **AUTORIZACION**	

OBJETIVO(S):

Que el alumno:

1. Conozca los conceptos y métodos avanzados usados en criptografía.

2. Sea capaz de implementar computacionalmente alguno de los algoritmos presentados fuera de un paquete de procesamiento simbólico.

CONTENIDO SINTETICO:

1. INTEGRIDAD DE LA INFORMACIÓN.

Presentación de la problemática.
Funciones hash.
Construcciones básicas y resultados generales.
Ataques a funciones hash.
Ejemplos de funciones hash (SHA1, MD5).

2. IDENTIFICACIÓN Y AUTENTIFICACIÓN.

Objetivos y aplicaciones.
Propiedades de protocolos de identificación.
Autentificación débil: claves (passwords).

CASA ABIERTA AL TIEMPO
UNIVERSIDAD AUTONOMA METROPOLITANA

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

CLAVE 213811	CRIPTOGRAFIA II

Autentificación fuerte: claves de uso único (one-time password).

3. FIRMAS DIGITALES.

Objetivos y aplicaciones.
Esquemas de la firma digital.
El RSA y firma digital.
Formatos: ISO/IEC 9796 y PKCS # 1.
Otros esquemas de firma digital (Fiat-Shamir, DSA, El Gamal, one-time).
Certificado y sobre digital.

4. ESTABLECIMIENTO Y MANEJO DE LLAVES.

Objetivos y propiedades.
Distribución de llaves basada en cifrados simétricos.
Distribución de llaves basada en cifrados asimétricos.
Distribución confidencial de llaves.

5. TEMAS OPTATIVOS.

Técnicas de implementación.
Aritmética de enteros de precisión múltiple. Aritmética modular de precisión múltiple. Algoritmos para obtener el MCD. Exponenciación.
Estándares.
Estándares usados en la banca (ANSI, ISO). Estándares usados en el gobierno estadounidense (FIPS).
Estándares usados en internet (RFCs). Estándares PKI´s.
Taller.
Usando PGP. Usando DES, AES, RSA.

MODALIDADES DE CONDUCCION DEL PROCESO ENSEÑANZA-APRENDIZAJE:

Los temas básicos del curso serán expuestos por el profesor. Los temas optativos serán expuestos por los alumnos ante el grupo. Se organizarán sesiones de discusión a manera de taller. El alumno realizará un proyecto final sobre alguno de los temas optativos que deberá tener un alto grado de dificultad computacional.

UNIVERSIDAD AUTONOMA METROPOLITANA
CASA ABIERTA AL TIEMPO

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

CLAVE 213811	CRIPTOGRAFIA II

MODALIDADES DE EVALUACION:

Al menos dos evaluaciones periódicas y/o una evaluación terminal: 60%.
Implementación computacional: 20%.
Elaboración de un reporte escrito sobre alguno de los temas opcionales y exposición oral: 20%.

BIBLIOGRAFIA NECESARIA O RECOMENDABLE:

1. Kaufman, Ch. et al., Network Security: Private Comunications in a pubic world, Prentice Hall PTR, 2nd ed., 2002.
2. Koblitz, N.I., A Course in Number Theory and Cryptography. Springer Verlag, 1994.
3. Daemen, J. & Rijmen, V., The Design of Rijndael. Information Security and Cryptography, Text and Monographs, Springer Verlag, 2002.
4. Menezes, A.J. et al., Handbook of Applied Cryptography. CRC Press, 1997, (http://www.carc.math.uwaterloo.ca/hac/).
5. Mollin, R. A., RSA and Public-Key Cryptography, Chapman & Hall, 2002.
6. Robling, D.E., Cryptography and Data Security. Addison Wesley, 1987.
7. Schneier, B., Applied Cryptography. John Wiley & Sons, 1997.
8. Stinson, D. R., Cryptography: Theory and Practice Chapman & Hall, 2nd ed., 2002.

UNIVERSIDAD AUTONOMA METROPOLITANA
CASA ABIERTA AL TIEMPO

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