C. 1997

(7) ✓

UNIVERSIDAD DE BUENOS AIRES
FACULTAD DE CIENCIAS EXACTAS Y NATURALES

1. DEPARTAMENTO: Computación

2. CUATRIMESTRE: Segundo de 1997.

3. ASIGNATURA: CRIPTOLOGIA

4. CARRERA: Licenciatura en Ciencias de la Computación

5. CARACTER DE LA MATERIA: Optativa

6. NUMERO DE CODIGO DE CARRERA: 18

7. NUMERO DE CODIGO DE MATERIA: C038

8. PUNTAJE: 3 puntos (planes 87 y 93)

9. PLAN DE ESTUDIOS AÑO: 1987 y 1993.

10. DURACION DE LA MATERIA: Cuatrimestral

11. HORAS DE CLASE SEMANAL:

a)TEORICAS 3 HS. c)PROBLEMAS 2 HS..
b)LABORATORIO d)SEMINARIOS

12. CARGA HORARIA TOTAL: 5 HORAS

13. ASIGNATURAS CORRELATIVAS: Algebra I y algoritmos y estructura de datos I

14. FORMA DE EVALUACION: Examen Final

15. PROGRAMA Y BIBLIOGRAFIA: Adjuntas a esta hoja

FECHA: 1/11/97

HS

Dr. Hugo Scolnik
Firma y Aclaración
del Profesor Titular

Firma del Director
y Sello Aclaratorio

Lic. IRENE LOISEAU
DIRECTORA
DEPTO. DE COMPUTACION
F. C. E. y N. UBA

FACULTAD DE CIENCIAS EXACTAS Y NATURALES - U. B. A. DEPARTAMENTO DE COMPUTACION

Criptología
segundo cuatrimestre 1997

Programa:

1. Criptografia clasica.
   Cifrados de corrimiento, substitucion, afin, Vigenere, Hilly de flujo.

2. Criptoanalisis.
   Criptoanalisis de los metodos afin, de substitucion y de Vigenere.

3. La teoria de Shannon.
   Teoria de la informacion. Teoria de la complejidad.
   Secreto perfecto. Entropia. Codificacion de Huffman y Entropia.
   Propiedades.

4. Algoritmos simetricos.
   Funciones univocas. Funciones de hashing.
   DES (Data Encryption Standard). Descripcion. Controversias.
   Criptoanalisis diferencial.
   Otros algoritmos de bloques. Criptografia de flujo.

5. Criptografia de clave publica.
   El problema de la distribucion de claves. Elementos de teoria de numeros. El algoritmo de Diffie-Hellman.
   Generacion probabilistica de numeros primos. Los metodos de Solovoy-Strassen y Rabin-Miller. Nuevos resultados sobre el error.
   El algoritmo RSA (Rivest-Adleman-Shamir). Ataques. Metodos de factorizacion.
   Implementacion computacional. Demostraciones de software.

6. Otros metodos de clave publica.
   El problema del logaritmo discreto. El algoritmo de ElGamal.
   Cuerpos finitos y curvas elipticas. Cuerpos de Galois.
   El problema de la mochila.

7. Firmas digitales y funciones de hashing.
   El algoritmo DSA (Digital Signature Algorithm).
   Las funciones MD4, MD5, y SHA. Time stamps. Implementaciones.
   Autoridades certificantes. Esquemas operativos.

8. Temas complementarios.
   Generacion de numeros aleatorios. Tests. Criptografia probabilistica.
   Time attacks.
   Pruebas de conocimiento cero.
   Politica de exportacion de Estados Unidos. Seguridad en Internet.

Bibliografia:

Douglas Stinson," Cryptography, Theory and Practice", CRC Press Inc., Florida, USA, 1995.
Bruce Schneier," Applied Cryptography", Second Edition, J.Wiley, 1996.

.

Dr. .Hugo Scolnik

Lic. IRENE LOISEAU
DIRECTORA
DEPTO. DE COMPUTACION
F. C. E. y N. UBA