


UNIVERSIDAD DE BUENOS AIRES
FACULTAD DE CIENCIAS EXACTAS Y NATURALES

1. DEPARTAMENTO: Computación
2. CUATRIMESTRE: Segundo de 2004.
3. ASIGNATURA: **Tecnología PKI-Criptografía de clave pública aplicada a la seguridad de transacciones via Internet**
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:
8. PUNTAJE: 1 punto
9. PLAN DE ESTUDIOS AÑO: 1993
10. DURACION: 1 semana
11. HORAS DE CLASE SEMANAL:
a) TEORICAS/PRACTICAS: 15 horas b) LABORATORIO: c) PRACTICAS:
12. CARGA HORARIA TOTAL: 15 horas
13. ASIGNATURAS CORRELATIVAS: **Conocimientos básicos de 1) álgebra (matrices, permutaciones, estructuras) 2) algoritmos y estructuras de datos**
14. FORMA DE EVALUACION: final
15. PROGRAMA Y BIBLIOGRAFIA:

Profesor
Dr. Armando Carratala


Dr. Enrique Carlos Segura
Director
Depto. de Computación
F. C. E. y N - UBA

15) PROGRAMA:

Introducción: Introducir al cursante en los fundamentos, estándares, arquitectura y principales aplicaciones de la tecnología PKI. Destinado a alumnos y profesionales vinculados a las ciencias de la computación, matemáticas o ingeniería, en particular aquellos que estén orientados a la seguridad informática.

Objetivos: Brindar conocimientos básicos e introductorios sobre las aplicaciones de la tecnología PKI

Programa: MODULO I : FUNDAMENTOS CRIPTOGRAFICOS

Fundamentos de criptografía aplicados en la tecnología PKI. Breves nociones de criptografía simétrica y asimétrica. Criptosistema Pohlig-Hellmann. Problemas de la factorización y del logaritmo discreto. Intercambio de claves Diffie-Hellmann. Criptosistema RSA. Criptosistema ElGamal. Firma digital. Algoritmo DSA. Principales ataques a los criptosistemas de clave pública.

MODULO II : ARQUITECTURA PKI

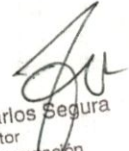
Definición de la tecnología PKI. Objetivo y métodos de la PKI. Arquitectura y Capas APKI. Modelo CDSA. Arquitectura y funcionalidad de la CryptoAPI Win32. Principales estándares soportados (X.509v3, SSLv3, IPsec, etc). Concepto de sesión SSL. Concepto de redes VPN. Presente y Futuro de la estandarización PKI.

MODULO III : APLICACIONES PKI

Concepto, clasificación y estructura de certificados digitales X.509. Concepto de Autoridad Certificante (AC). Modelos y cadenas de confianza. Certificación de Web Servers. Certificados digitales. Obtención de certificados: el enrollment. Certificados de atributos. El mercado actual de AC. Legislación de Firma Digital en la República Argentina. El futuro de la tecnología PKI.

16) BIBLIOGRAFIA:

Apunte de cátedra. No fue adjuntada otra bibliografía por parte del docente a cargo.


Dr. Enrique Carlos Segura
Director
Depto. de Computación
F. C. E. y N - UBA