



UNIVERSIDAD NACIONAL DE LA PLATA  
FACULTAD DE INFORMÁTICA

---

**SEGURIDAD Y PRIVACIDAD EN  
REDES**

**Año 2008**

Carrera: ***Licenciatura en Sistemas***  
**Planes 2003 y 2007.**

Año: ***Optativa***

Duración: ***Semestral***

Profesor: ***Lic. Javier Díaz***

Hs semanales: 6 hs

---

**Programa**

Definiciones básicas de seguridad y seguridad en Redes, Identificación de Problemas, Niveles de Seguridad. Identificando los ataques. Problemas frecuentes: en servicios.

Ataques comunes, Un ejemplo: servicio rechazado.

Prevención de Posibles ataques: UDP, SMURF, ICMP, Source Routing, Source Address Spoofing, IP Hijacking, TCP Sequence Number Prediction, Ventajas de la criptografía.

Herramientas y enfoques de la seguridad, Firewalls, Filtros y gateways.

Bastiones, Gateways tipo PROXY, Tuneles.

Criptografía clásica, Cifrados por substitución y por transposición; Pads.

Algoritmos computacionales, Claves simétricas y públicas.

Firma digital, Firma y secreto. Autenticación, Ataques por Criptoanálisis.

Seguridad de criptosistemas.

Esquema DES, Triple DES e idea; Diffie-Hellman y Diffie-Hellman entre n participantes, RSA.

Privacidad, cookies, sistema para asistir al usuario, Sellos de confianza.

**Bibliografía:**

***Libros:***

- "Cryptography and Data Security", Denning, 1982.
- "Network Security", Kaufman, Perlman & Speciner, 1995.
- "Network and Internetwork Security", William Stallings, 1995.
- "Building Internet Firewalls" Chapman & Zwicky, 1995.
- "IPSec: the new security standard for the Internet, intranets, and virtual private networks" Doraswamy, Naganand, 1999.



***Artículos:***

- "The Rijndael Block Cipher", Daemen & Rijmen.
- "Password Security: A Case History", Robert Morris and Ken Thompson, CACM Nov.1979, Vol. 22, Num. 11
- "UNIX Password Security - Ten Years Later", David Feldmeier and Philip Karn, Crypto89
- "The Keyed-Hash Message Authentication Code (HMAC)"

***Material en línea:***

- Kerberos in Windows 2000
- RFC 1760: The S/KEY One-Time Password
- The Internet Worm Program: An Analysis
- Tour of the worm
- Securing IP
- IPSEC Internet drafts
- "The Keyed-Hash Message Authentication Code (HMAC)"