Universidad Técnica Federico Santa María
Escuela de Graduados

ASIGNATURA: **CRIPTOGRAFÍA**			SIGLA: **IPD-442**
PRERREQUISITOS: Probabilidades y Procesos Aleatorios (ELO-204)			CREDITOS: **4**
HRS.CAT.SEM.: **3**	HRS.AYUD.SEM.:	HRS.LAB.SEM.:	EXAMEN: **NO**

OBJETIVOS:

1. Conocer, utilizar correctamente y analizar la seguridad de las primitivas criptográficas
2. Comprender cómo se utilizan correctamente las primitivas criptográficas y analizar la seguridad de protocolos como dinero digital y sistemas de elecciones on-line.

METODOLOGIA:

- Clases expositivas, estudio artículos científicos, ejercicios.

CONTENIDOS:

- Primitivas criptográficos:
  - Stream ciphers: principios, one time pad, random numbers generators.
  - Block ciphers: principios, DES and AES, exhaustive key search attacks, modes of operation.
  - Public key cryptography: practical aspects, number theory y RSA.
  - Firmas digitales: servicios de seguridad, principios, la firma RSA.
  - Hash functions: motivación, seguridad de los hash functions, algoritmo SHA-1.
  - Message Authentication Codes (MACs): principios, MACs con hash functions, MACs con block ciphers.
  - Key establishment: key establishment techniques, certificados digitales, infraestructura de clave pública, autoridad de certificación.
- Protocolos criptográficos:
  - Elección on-line
  - Dinero digital

BIBLIOGRAFIA:

1. "Cryptography Engineering: Design Principles and Practical Applications", Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. Wiley Publishing, 2010.
2. "Understanding Cryptography: A Textbook for Students and Practitioners", Christof Paar, Jan Pelzl, Springer, 2010.

Elaborado :	Daniel Caragata	Observaciones:
Aprobado :	Depto. Electrónica – D.G.I.P.	Última actualización:
Fecha :	Agosto 2014	