UNIVERSIDAD DEL BIO-BIO
VICERRECTORIA ACADEMICA – DIRECCION DE DOCENCIA

ASIGNATURA : CRIPTOGRAFIA

CÓDIGO : 63xxxx

I. IDENTIFICACIÓN

1.1 CAMPUS : CHILLÁN

1.2 FACULTAD : CIENCIAS EMPRESARIALES

1.3 UNIDAD : DEPARTAMENTO CIENCIAS DE LA COMPUTACIÓN Y TECNOLOGÍAS DE INFORMACIÓN

1.4 CARRERA : INGENIERÍA CIVIL EN INFORMÁTICA

1.5 Nº CRÉDITOS : 3

1.6 TOTAL DE HORAS: 04 HT: 02 HP: 02 HL:

1.7 PREQUISITOS DE LA ASIGNATURA:

- ANALISIS Y DISEÑO DE ALGORITMOS, 634073
- ALGEBRA II, 240036

II. DESCRIPCIÓN

En esta asignatura se estudian los elementos básicos de la criptografía moderna y se analizan los algoritmos y protocolos del área, tanto desde una perspectiva general como orientada a aplicaciones en dominios particulares (seguridad informática, criptoanálisis etc). Se parte con un estudio matemático de la teoría de números atingente al ramo. Se espera que al finalizar el curso el alumno haya adquirido las competencias básicas o fundamentales para la criptografía moderna.

III. OBJETIVOS

a) Generales:

Adquirir los conocimientos de la teoría de números necesarios para la criptografía moderna. Comprender y ser capaz de implementar los algoritmos y protocolos básicos para problemas de seguridad informática.

b) Específicos

- Conocer la teoría de números elemental, principalmente lo relativo a la teoría de las congruencias.
- Comprender protocolos criptográficos básicos (RSA, Diffie-Hellman, etc).
- Adquirir nociones de las dificultades asociadas al criptoanálisis (el problema de la factorización de enteros, tests de primalidad etc).
- Adquirir nociones de tópicos varios de criptografía (voto electrónico, firma electrónica, protocolos zero-knowledge etc).

IV. UNIDADES PROGRAMÁTICAS

UNIDADES	HORAS
Unidad 0: Qué es la Criptografía Moderna	10
Unidad 1: Teoría de Números Elemental	20
Unidad 2: Protocolos Básicos	20
Unidad 3: Criptoanálisis, Factorización de Enteros, Primalidad	20
Unidad 4: Otros Tópicos de Criptografía	10
TOTAL:	80

V. CONTENIDO UNIDADES PROGRAMÁTICAS

UNIDADES	CONTENIDO
Unidad 0: Qué es la criptografía moderna.	Breve repaso de la criptografía en la historia. La necesidad de una aproximación científica a esta disciplina.
Unidad 1: Teoría de números elemental.	- Números primos y compuestos, algoritmo de Euclides. - Congruencias. - Teoremas de Fermat y Euler. Símbolo de Legendre.

Unidad 2: Protocolos básicos.	- Conceptos de clave pública y privada. - Protocolo RSA de encriptación. - Protocolo Diffie-Hellman de generación segura de claves.
Unidad 3: Criptoanálisis, factorización de enteros, primalidad.	- Cómo quebrar (en teoría) protocolos criptográficos. - Algoritmos de factorización de enteros: método Rho de Pollard. - Tests de Primalidad (test de Fermat, Miller-Rabin, Lehman-Peralta).
Unidad 4: Otros tópicos de criptografía.	- Voto electrónico. - Protocolos zero-knowledge. - Firma digital. - Otros.

VI. METODOLOGÍA

- Clases expositivas.
- Trabajo grupal.

VII. TIPOS DE EVALUACIÓN (PROCESO Y PRODUCTO)

- Trabajo de investigación.
- Certámenes.

VIII. BIBLIOGRAFÍA:

a) Básica

- Koblitz, Neal: A Course in Number Theory and Cryptography. Springer Verlag, 1993. Second Edition.
- Vinográdov, Ivan: Fundamentos de la Teoría de los Números. Editorial Mir (Moscú), 1971.
- Schneier, Bruce: Applied Cryptography. Wiley, 1996.

b) Complementaria

- Cohen, Henri: A Course in Computational Algebraic Number Theory. Springer Verlag, 2000.
- Yan, Song: Number Theory for Computing. Springer Verlag, 2000.
- Knuth, Donald: The Art of Computer Programming, volumen 2, Seminumerical Algorithms. Addison Wesley, 1998.