Estrutura Curricular (EC)

Formulário nº 13 – *Especificação da Disciplina/Atividade*

Conteúdo de estudos: Matemática

Nome da Disciplina/Atividade	**Código**	Criação (X)
Criptografia	VMA00038	Alteração: nome ( ) CH ( )

Departamento/Coordenação de Execução: Departamento de Matemática

Carga Horária total: 60h Teórica: 60h Prática: 0h Estágio: 0h

Disciplina/Atividade: Obrigatória ( ) Optativa (X) AC ( )

Objetivos da Disciplina/Atividade:

O objetivo deste curso é apresentar ao aluno as bases históricas e conceituais da criptografia e utilizar conceitos de Teoria dos Números para estudar o método de criptografia de chaves públicas conhecido como RSA.

Descrição da Ementa:

Criptografia e segurança em rede. Serviços e Modelos de Segurança em rede. Criptografia da antiguidade à idade moderna. Noções de lógica. Números primos e algoritmo da divisão. O algoritmo de Euclides. Aritmética modular. O teorema de Fermat. Testes de primalidade. Teorema de Euler. Teorema Chinês dos restos. RSA. Logaritmo discreto e Aplicações.

Bibliografia Básica:

1. COUTINHO, S.C. *Números inteiros e Criptografia RSA*. (Coleção Matemática e Aplicações) 2 .ed. Rio de Janeiro: IMPA, 2013.
2. COELHO, S. P., MILIES, C.P. *Números: Uma Introdução à Matemática*. 1. ed. São Paulo: EDUSP, 1998.
3. SANTOS, J. P. de O. *Introdução à Teoria de Números*. (Coleção Matemática Universitária) Rio de Janeiro: IMPA, 1998.

Bibliografia Complementar:

1. HEFEZ, A. *Curso de Álgebra*. (Coleção Matemática Universitária) v. 1. Rio de Janeiro: IMPA, 1997.
2. SANTOS, J. P. de O. *Introdução à Teoria de Números*. (Coleção Matemática Universitária) Rio de Janeiro: IMPA, 1998.
3. GONÇALVES, A. Introdução à Álgebra. Rio de Janeiro: IMPA, 1999.
4. STINSON, D. R. *Cryptography: theory and practice*. New York: CRC Press, 1995.
5. TKOTZ, V. *Criptografia - Segredos Embalados para Viagem*. 1. ed. Novatec Editora, 2005.

_____ _____

Coordenador de Curso Chefe de Departamento

Data _____/_____/_____ Data _____/_____/_____