FGV EMAp
ESCOLA DE MATEMÁTICA APLICADA

CURSO: Graduação em Matemática – 2º semestre de 2016
DISCIPLINA: Álgebra, Números e Criptografia
PROFESSOR(ES): Moacyr Alvim
CARGA HORÁRIA: 60h
PRÉ-REQUISITO: Matemática Discreta
HORÁRIO E SALA DE ATENDIMENTO:
segunda-feira: 10h a 12h.
SALA: 312

COMPLEMENTAÇÃO DE CARGA HORÁRIA: 4 aulas de 1h40min

PLANO DE ENSINO

1. Ementa

Algoritmo euclideano; Fatoração única, algoritmo de Fermat, primos, Mersenne e Fermat, Crivo de Eratóstenes; Aritmética modular, Critérios de divisibilidade, Equações diofantinas; Divisão modular; Pequeno teorema de Fermat; Pseudoprimos; Sistemas de congruências; Partilha de senhas; Grupos; Teorema de Lagrange; Mersenne e Fermat ; Raízes primitivas; Criptografia RSA.

2. Objetivos da disciplina

O objetivo da disciplina é ampliar, a partir do conhecimento e habilidades desenvolvidas em Matemática Discreta, a capacidade de aplicação de propriedades aritméticas e algébricas dos números inteiros em diversos processos envolvendo segurança na transmissão de dados. Em torno ao método de Criptografia RSA serão estudados conceitos e teoremas da matemática pura que encontram diversas aplicações também em outras áreas do conhecimento. Espera-se que os alunos obtenham um primeiro contato instrutivo com Teoria dos Números e Álgebra Abstrata, mas especificamente Teoria dos Grupos, entendendo suas principais aplicações e permitindo o posterior aprofundamento conforme interesse e necessidade.

3. Procedimentos de ensino (metodologia)

Para a parte teórica, seguiremos como livro texto "Números Inteiros e Criptografia RSA", de S. C. Coutinho. Os conceitos e teoremas mais importantes serão comentados em aula, sendo recomendada a leitura prévia dos capítulos. Serão propostas abundantes listas de exercícios para trabalho individual e em grupo, com espaço em sala de aula para resolução de dúvidas. As listas incluirão implementações computacionais de algoritmos importantes na prática.

4. Conteúdo programático detalhado

Datas	Tópico
25 a 29/07	Introdução à Criptografia
01 a 05/08	Divisão Euclidiana, Fatoração Única
24/08	Aritmética Modular
29 a 31/08	Equações Diofantinaas
05 a 09/09	Teorema de Fermat
12 a 16/09	Exercícios
19 a 23/09	Sistemas de Congruências
26 a 30/09	Exercícios
01 a 08/10	Semana da A1
10/10	Pseudoprimos
17 a 21/10	Grupos
24 a 28/10	Grupos – Teorema de Lagrange
31/10 a 4/11	Mersenne e Fermat, Teste de Lucas-Lehmer
07 a 11/11	Raízes primitivas
16/11	Criptografia RSA
21 a 25/11	Exercícios
28 a 30/11	Exercícios
01 a 08/12	Semana da A2
14 a 21/12	Semana da AS

5. Procedimentos de avaliação

As notas da A1 e da A2 serão compostas pela prova teórica (70%) e por trabalhos teóricos e computacionais realizados individualmente e em grupo (30%).

6. Bibliografia Obrigatória

Coutinho, S. Collier. Números Inteiros e Criptografia. Coleção Computação e Matemática. IMPA

Hefez, Abramo. Elementos de Aritmética. SBM.

Gonçalves, Adilson. Introdução a Álgebra. IMPA.

7. Bibliografia Complementar

Codes and Ciphers: Julius Caesar, the Enigma, and the Internet R. F. Churchhouse;

An Introduction to Cryptography Richard A. Mollin;

RSA and Public-Key Cryptography Richard A.

A Course in Number Theory and Cryptography NEAL Koblitz;

Algebraic Aspects of Cryptography NEAL Koblitz.

8. Minicurrículo do(s) Professor(s)

Possui mestrado em Matemática pela Associação Instituto Nacional de Matemática Pura e Aplicada (1998) e doutorado em Matemática pela Associação Instituto Nacional de Matemática Pura e Aplicada (2004). Atualmente é professor da Fundação Getúlio Vargas. , atuando principalmente nos seguintes temas: geometria diferencial discreta, eixos de simetria de figuras, redes complexas, teoria dos jogos e modelos baseados em agentes.

9. Link para o Currículo Lattes

http://lattes.cnpq.br/9077049649454688