UNIVERSIDADE FEDERAL DO ESTADO DO RIO DE JANEIRO
CENTRO DE CIÊCIAS EXATAS E TECNOLOGIA (CCET)
ESCOLA DE MATEMÁTICA

PROGRAMA DE DISCIPLINA

CURSO: Licenciatura em Matemática

DEPARTAMENTO: Matemática e Estatística (DME)

DISCIPLINA: Introdução à Criptografia

PRÉ-REQUISITO: Teoria dos Números

CARGA HORÁRIA: 60 h **NÚMERO DE CRÉDITOS:** 4 **CÓDIGO:**

EMENTA: Revisão de Teoria dos Números. Criptografia em chave pública: introdução, método, segurança e assinatura no RSA.

OBJETIVOS DA DISCIPLINA: Fornecer ao aluno a base matemática necessária ao entendimento e aplicação de um dos métodos de criptografia mais usados em aplicações comerciais, o RSA.

CONTEÚDO PROGRAMÁTICO:

- **Unidade 1:** Teoria dos números
  Algoritmo de Euclides
  Teorema da Fatoração única
  Números primos
  Números de Mersenne
  Números de Fermat

- **Unidade 2:** Aritmética modular
  Inteiros módulo n
  Potências
  Equações Diofantinas
  Divisão modular

- **Unidade 3:** Criptografia RSA
  Pré-codificação
  Codificando e decodificando
  Segurança
  Assinaturas

AVALIAÇÃO: Os critérios de avaliação envolvem: a apreensão mínima dos conhecimentos tratados no curso, a participação e assiduidade. Os procedimentos de avaliação contemplam provas escritas de conhecimentos, que poderão, eventualmente, ser combinadas com (ou substituídas por) testes, trabalhos individuais ou em grupo, listas de exercícios resolvidas ou seminários.

BIBLIOGRAFIA:

Básica

- COUTINHO, C. *Números inteiros e criptografia RSA*. Série de Computação e Matemática. Rio de Janeiro: IMPA, 2005.
- POLCINO, C. *Números: uma introdução à Matemática*. São Paulo: Edusp, 2003.
- SANTOS, J.P. *Introdução à Teoria dos Números*. Coleção Matemática Universitária. Rio de Janeiro: IMPA, 2009.

Complementar

- KOBLITZ, N. *A course in number theory and cryptography*. Graduate Texts in Mathematics 97, Springer-Verlag, 1987.