UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO

Rua Dom Manoel de Medeiros, s/n. - Dois Irmãos 52171-900 Recife - PE
Fone: 0xx-81-3302-1000 www.ufrpe.br

PROGRAMA DE DISCIPLINA

IDENTIFICAÇÃO			
DISCIPLINA: **CRIPTOGRAFIA**			CÓDIGO:
DEPARTAMENTO: **MATEMÁTICA**			ÁREA: **MATEMÁTICA**
CARGA HORÁRIA TOTAL: **60horas**			NÚMERO DE CRÉDITOS: **4**
CARGA HORÁRIA SEMANAL-	TEÓRICAS: **4**	PRÁTICAS: - ..	TOTAL: **4**
PRÉ-REQUISITOS: **INTRODUÇÃO À ÁLGEBRA**			
CO-REQUISITOS: -			

OBJETIVOS

Apresentar ao nosso aluno uma introdução à teoria geral da Criptografia de chave privada e de chave pública, explorando a criptografia RSA, um dos modelos de criptografia mais utilizados na atualidade, cuja base matemática é a Aritmética dos Inteiros. O aluno deverá ser estimulado a desenvolver atividades voltadas para sua futura atuação como professor, que agucem o espírito crítico, a criatividade e a autoconfiança por meio de sua participação ativa.

EMENTA

Criptografia. Congruências. Criptografia RSA.

CONTEÚDOS

1. Criptografia.
Teoria geral de criptografia de chave pública e privada.

2. Conguências.
Teoremas de Fermat e Gauss. Teorema chinês dos Restos. Raízes Primitivas.

3. Criptografia RSA.
Pré-codificação, codificação e decodificação. Segurança.

4. Outros modelos de criptografia.

BIBLIOGRAFIA

COUTINHO, S. C. *Números Inteiros e Criptografia RSA*. IMPA.