



MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
SECRETARIA GERAL DOS CONSELHOS DA ADMINISTRAÇÃO SUPERIOR
CONSELHO DE ENSINO, PESQUISA E EXTENSÃO

RESOLUÇÃO Nº 324/2011

EMENTA: Aprova criação da disciplina intitulada: “CRIPTOGRAFIA”, como optativa, na grade curricular do Curso de Licenciatura em Matemática do Departamento de Física e Matemática desta Universidade.

O Presidente do Conselho de Ensino, Pesquisa e Extensão da Universidade Federal Rural de Pernambuco, no uso de suas atribuições e tendo em vista o disposto no Parágrafo 6º do Art. 15 do Estatuto desta Universidade e considerando os termos da Decisão Nº 058/2011 da Câmara de Ensino de Graduação deste Conselho, em sua II Reunião Extraordinária, realizada no dia 23 de novembro de 2011, exarada no Processo UFRPE Nº 23082.013382/2010,

R E S O L V E:

Art. 1º - Aprovar, em sua área de competência, a criação da disciplina intitulada: “CRIPTOGRAFIA”, com carga horária total de 60 (sessenta) horas/aula, como optativa, na grade curricular do Curso de Licenciatura em Matemática, do Departamento de Física e Matemática desta Universidade, cujo Programa de Disciplina encontra-se em anexo, conforme consta do Processo acima mencionado.

Art. 2º - Revogam-se as disposições em contrário.

SALA DOS CONSELHOS DA UFRPE, em 28 de novembro de 2011.

PROF. VALMAR CORRÊA DE ANDRADE
= PRESIDENTE =

Confere com o original assinado pelo Reitor e arquivado nesta Secretaria Geral.



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: CRİPTOGRAFIA	CÓDIGO:
DEPARTAMENTO: MATEMÁTICA MATEMÁTICA	ÁREA:
CARGA HORÁRIA TOTAL: 60horas CRÉDITOS: 4	NÚMERO DE
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 voltados para sua futura atuação como professor que estimulem 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. Congruências.
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.

Emissão

Data:

Responsável: