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: **06010**	
DEPARTAMENTO: **MATEMÁTICA**	ÁREA: **MATEMÁTICA**	
CARGA HORÁRIA TOTAL: **60 h**	NÚMERO DE CRÉDITOS: **4**	
CARGA HORÁRIA SEMANAL: **4 h**	TEÓRICAS: 4**h**	PRÁTICAS: **0h**
PRÉ-REQUISITOS: **NENHUM**		
CO-REQUISITOS: **NENHUM**		
SEMESTRE/ANO DE APLICAÇÃO:		

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. Testes de primalidade

5. Outros modelos de criptografia.

BIBLIOGRAFIA

BIBLIOGRAFIA BÁSICA:
[1] BUCHMANN, Johannes A.. Introdução à Criptografia. Editora Berkeley, São Paulo, 2002.
[2] COUTINHO, S. C. Números Inteiros e Criptografia RSA, IMPA/SBM, Rio de Janeiro, 1997.
[3] SHOKRANIAN, Salahoddin. Criptografia para Iniciantes. Ciência Moderna, 1ª edição, 2005.

BIBLIOGRAFIA COMPLEMENTAR:

[1] HOFFSTEIN, Jeffrey, PIPHER, Jill & SILVERMAN, Joseph H.An Introduction to Mathematical Cryptography. Springer, 2008.
[2] MENEZES, A.J.; VANSTONE, S.A.; van OORSCHOT, A.C. "Handbook of Applied Cryptography", CRC Press, 2001.
[3] RIESEL, Hans. Prime Numbers and Computer Methods for Factorization, volume 126 of Progress in Mathematics. Birkhäuser, 2nd edition, 1994.
[4] SINGH, Simon. O Livro dos Códigos. 7ª Ed. Editora Record. Rio de Janeiro, 2008.
[5] TKOTZ, Viktoria. CRIPTOGRAFIA - Segredos Embalados para Viagem. Editora NOVATEC, São Paulo, 2005.

Emissão
Data: Responsável: