Universidade Federal de Pernambuco
Pró-Reitoria de Pesquisa e Pós-Graduação
Diretoria de Pós-Graduação

PROGRAMA VÁLIDO PARA O SEMESTRE DE

PROGRAMA DE DISCIPLINA

DADOS DA DISCIPLINA

CÓDIGO	NOME	CARGA HORÁRIA SEMANAL TEÓRICA	CARGA HORÁRIA SEMANAL PRÁTICA	N.º DE CREDITOS	CARGA HORÁRIA GLOBAL
IN1113	**Fundamentos da Criptografia Moderna**	**4**	**0**	**4**	**60**

PRÉ – REQUISITOS

Nenhum

EMENTA

Abordagem moderna: seguranca demonstrável.

Esquemas criptograficos versus ataques.

Encriptacao (simetrica; assimétrica; cifras de bloco; cifras de fluxo).

Troca de chaves.

Geracao (pseudo)aleatória de chaves.

Autenticacao de mensagens (funções "hash").

Criptografia de chave pública.

Assinaturas digitais.

CONTEÚDO PROGRAMÁTICO

BIBLIOGRAFIA BÁSICA

1. Lecture Notes on Cryptography, S. Goldwasser and M. Bellare, 2001.
(This is a set of lecture notes for a summer course on cryptography, taught by the authors at the Massachusetts Institute of Technology (MIT), 1996--2001.)
(http://www-cse.ucsd.edu/users/mihir/papers/gb.pdf)

2. Introduction to Modern Cryptography, Mihir Bellare and Phillip Rogaway.
(Functions as course notes for UCSD course CSE207. Feedback, corrections and comments welcome.) (http://www-cse.ucsd.edu/users/mihir/cse207/)

3. Foundations of Cryptography - Basic Tools, Oded Goldreich.
Cambridge University Press, June 2001.

CURSO A QUE PERTENCE A DISCIPLINA

Mestrado e Doutorado em Ciência da Computação

HOMOLOGADO PELO COLEGIADO DE CURSO

Em 20 de agosto de 2008

_____
ASSINATURA DO COORDENADOR DO CURSO

_____
ASSINATURA DA SECRETÁRIA