UNIVERSIDADE ESTADUAL DE SANTA CRUZ-UESC
PRÓ-REITORIA DE GRADUAÇÃO – PROGRAD
DEPARTAMENTO DE CIÊNCIAS EXATAS -DCET
COLEGIADO DE CIÊNCIA DA COMPUTAÇÃO-COLCIC

PROPOSTA DE PROGRAMA DE DISCIPLINA

CÓDIGO	DISCIPLINA	PRÉ-REQUISITOS
CET 111	Tópicos Avançados de Computação I – Criptografia	Álgebra Abstrata Estrutura de dados

C/HORÁRIA		CRÉDITOS	PROFESSOR (A)
T	30	2	**César Alberto Bravo Pariente**
P	30	1	
TOTAL	60	3	

EMENTA

Introdução: Técnicas clássicas de criptografia não digital. Teoria de números e Teoria da informação. Criptografia simétrica. Criptografia assimétrica. Autenticação e identificação. Assinatura digital. Funções de espalhamento.

OBJETIVOS

Atualizar o aluno em tópicos atuais relativos a área de Criptografia digital.

METODOLOGIA

Aulas expositivas e desenvolvimento de projetos de software exercitando os conceitos da disciplina.

AVALIAÇÃO

Prova teóricas e projetos de software.

CONTEÚDO PROGRAMÁTICO	

Teoria de números, Teoria da informação, Criptografia e Criptoanalise.
Grupo, anel e corpo
Soma e produto mod n
Algoritmo de Euclides de mdc
Problema de sigilo e autenticidade
Tipos de criptoanalise: frequencia, substituição, composição.
Difusão e confusão
Entropia
Segurança perfeita
Criptosistema aleatório

Criptografia simétrica.
DES : Data Encryption Standard
IDEIA : International Data Encryption Algorithm
SAFER : Secure and Fast Encryption Routine
RC5 e RC6
FEAL : Fast Encryption Algorithm
AES : Advanced Encryption Standard
CD : Criptanálise diferencial
CL : Criptanálise linear
Fortalecimento contra CD e CL
Modos de operação

Criptografia assimétrica.
Problema de logaritmo discreto
Intercambio de chaves simêtricas Diffie Hellman
Algoritmo RSA
Algoritmo Rabin
Algoritmo ElGamal
Problema de logaritmo discreto geral
Algoritmo ElGamal geral
Curvas Elipticas
Algoritmo MH

Autenticação e identificação
Jogo de cara e coroa por telefone
Protocolo de Feige, Fiat e Shamir
Protocolo de identificação GQ
Protocolo de Schnorr

Assinatura Cryptografica
Assinatura RSA

Algoritmo Rabin de assinatura
Assinatura Feige-Fiat-Shamir
Esquema de assinatura GQ
Algoritmo ElGamal de assinatura
Algoritmo DSS : Digital Signature Standard
Algoritmo Schnorr de assinatura

Funções de Espalhamento
Método Merkle-Damgård
Ataque pelo Paradoxo de Aniversário
Little-endian e big-endian
Algoritmo MD4.
Algoritmo MD5.
Algoritmo SHA - Secure Hash Algorithm
Futuro da funções de espalhamento

REFERÊNCIA BIBLIOGRÁFICA

1. Routo Terada Segurança de Dados. Criptografia em rede de computador. 2ª Edição Revista e Ampliada. ISBN: 9788521204398. Editora Blucher, 2008. 312 páginas.
2. Alfred J. Menezes, Paul C. van Oorschot and Scott A. Vanstone. Handbook of Applied Cryptography. CRC Press. ISBN: 0-8493-8523-7. October 1996, 816 pages. Fifth Printing (August 2001).