MINISTÉRIO DA EDUCAÇÃO

CENTRO FEDERAL DE EDUCAÇÃO TECNOLÓGICA CELSO SUCKOW DA FONSECA
CAMPUS PETRÓPOLIS

CURSO SUPERIOR DE ENGENHARIA DE COMPUTAÇÃO

DEPARTAMENTO		PLANO DE CURSO DA DISCIPLINA
ENGENHARIA DE COMPUTAÇÃO		**CRIPTOGRAFIA**

CÓDIGO		PERÍODO		ANO		SEMESTRE		PRÉ-REQUISITOS
GCOM0081PE				2015		1		1. Algoritmos e Estruturas de Dados I.
CRÉDITOS		AULAS/SEMANA				TOTAL DE AULAS NO SEMESTRE		
		TEÓRICA	PRÁTICA	ESTÁGIO				
4		2	2	0		72		

EMENTA

1. História da Criptografia.
2. Teoria dos Números.
3. Estruturas Algébricas.
4. Criptografia a Simétrica.
5. Assimétrica.
6. Funções de Hash.
7. Assinatura digital.
8. Criptografia a Pós-Quântica.
9. Criptoanálise e Ataques.

BIBLIOGRAFIA

Básica:

1. MENEZES, A.J.; VAN OORSCHOT, P.C.; SCOTT, A. Vanstone, Handbook of Applied Cryptography. CRC Press, 1996.
2. STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. 4a ediçãao. São Paulo: Pearson, 2008.
3. TERADA, R. Segurança de dados: criptografia a em redes de computador. 2a edição revista e ampliada. São Paulo: Bluncher, 2008.

Complementar:

1. SCHENEIER, B. Applied Cryptography Protocols, Algorithms, and Source Code in C. John Wiley & Sons, 1996.
2. SHOKRANIAN, S. Teoria dos números. Editora Unb, 1999.
3. FERGUSON, N.; SCHENEIER, B. Practical Cryptography. Wiley, 2003.
4. BERNSTEIN, D.J. Post-Quantum Cryptography. Springer, 2009.

5. HANKERSON, D.; MENEZES, A.J.; VANSTONE, S. Guide to Elliptic Curve Cryptography. Springer, 2003.

OBJETIVOS GERAIS

O objetivo da disciplina é apresentar ao aluno as diferentes técnicas de soluções numéricas utilizadas em diversas áreas da engenharia. Além disso o aluno poderá avaliar a eficiência e convergência dos métodos apresentadas

METODOLOGIA

Cada aula consistirá na combinação adequada de:

- Exposição detalhada de elementos necessários para o entendimento dos métodos e conceitos.
- Exercícios, atividades e estudos de casos, de forma individual ou em grupo.
- Trabalhos práticos de implementação das técnicas ensinadas.
- Provas individuais.

CRITÉRIO DE AVALIAÇÃO

A avaliação será feita através de duas provas teórica, correspondendo a 80% da nota final e dois trabalhos práticos, juntamente com seu relatório correspondendo a 20% dos pontos da disciplina.

CHEFE DO DEPARTAMENTO	
NOME	ASSINATURA
Laura Silva de Assis	

PROFESSOR RESPONSÁVEL PELA DISCIPLINA	
NOME	ASSINATURA
Pedro Carlos da Silva Lara	

APROVADO PELO CONSELHO DEPARTAMENTAL EM: ____/____/____

CONTEÚDO PROGRAMÁTICO

1. História da Criptografia.
   1. Cifra de Cesar
   2. Cifra de Vigenere
   3. Cifra de Vernan

4. One Time Pad
5. Teoria da Informação
6. Entropia

2. Teoria dos Números.
    1. Estruturas Algébricas
    2. Grupos
    3. Aneis
    4. Corpos
    5. Corpos Finitos
    6. Corpo de Gailos

3. Criptogra a Simétrica.
    1. DES
    2. AES
    3. Modos de Criptografia
    4. CBC
    5. ECB

4. Assimétrica.
    1. RSA
    2. ElGamal
    3. Diffie Helman
    4. Curvas Elípticas

5. Funções de Hash.
    1. Funções de Hash Segura
    2. Construção de Hash
    3. MD5
    4. SHA1
    5. SHA2

6. Assinatura digital.
    1. DSS
    2. DSA

7. Criptogra a Pós-Quântica.
    1. Multivariaveis Quadráticas

8. Criptoanálise e Ataques.
    1. Criptoanálise Linear
    2. Criptoanálise Diferencial