Universidade Federal de Santa Catarina
Centro Tecnológico
Departamento de Informática e Estatística
Programa de Pós-Graduação em Ciência da Computação

Plano de Ensino

1) Identificação

Disciplina: Criptografia e Segurança em Redes de Computadores
Carga horária: 45 horas/aula
Professora: Ricardo Felipe Custódio

2) Requisitos: não há.

3) Ementa:

Criptografia Simétrica e Assimétrica. Ciclo de vida de chaves simétricas e assimétricas. Controle de Acesso. Integridade de dados. Autenticação. Assinatura Digital. Protocolos Criptográficos. Protocolos Seguros de Comunicação. Códigos Maliciosos.

4) Objetivos:

Geral: Compreender os principais problemas existentes e possíveis soluções de criptografia e segurança em redes de computadores.

Específicos:

- Compreender criptografia e protocolos criptográficos e o ciclo de vida de chaves criptográficas;
- Mostrar os conceitos e principais métodos de autenticação, integridade e assinatura digital;
- Identificar os principais mecanismos de códigos maliciosos e métodos de proteção;
- Apresentar os mais importantes protocolos criptográficos e de comunicação segura.

5) Conteúdo Programático:

6.1) Exame detalhado da criptografia convencional e princípios de projeto [20 horas-aula]
- Revisão de estruturas de matemática discreta aplicada a criptografia
- Introdução a criptografia simétrica e gestão de chaves criptográficas
- Introdução a protocolos criptográficos

6.2) Métodos de Autenticação e de controle de Integridade [10 horas-aula]

- Controle de Acesso
- Kerberos, X.509, IBE
- Integridade e Funções Hash

6.3) Assinatura Digital [10 horas-aula]
- Principais algoritmos de assinatura digital

6.5) Aplicações
- PGP

6) Metodologia:

As aulas serão expositivas, intercaladas com algumas aulas práticas. Também serão passados aos alunos alguns artigos científicos clássicos sobre os temas tratados.

7) Avaliação

Serão feitas duas provas teóricas (P1 e P2), um conjunto de até seis trabalhos individuais (TI).

A média final (MF) será dada por: MF = (P1 + P2 + TI)/3

Onde:

P1: Nota da Primeira Prova
P2: Nota da Segunda Prova
TI: Nota da médias dos trabalhos individuais

O conceito do aluno na disciplina será definido a partir da média final utilizando-se da tabela de equivalência abaixo:

Conceito	Significado	Nota
A	Excelente	9,0 –10,0
B	Bom	8,0 – 8,9
C	Regular	7,0 – 7,9
D	Insuficiente	< 7,0
I	Incompleto	---

Será considerado aprovado o aluno que obtiver conceito final igual ou superior a "C" e freqüência igual ou superior a 75% da carga horária da disciplina, obtendo os créditos equivalentes da disciplina.

8) Cronograma:

9) Bibliografia:

- **Bibliografia Básica**

- Stallings, William. Cryptografhy and Network Security: Priciples and Practice. Prentice Hall, 1999.569p.

- **Bibliografia Complementar**

- Menezes, Alfred J.; Oorschot, Paul C.; Vanstone, Scott A. Handbook of Applied Cryptography. New York: CRC Press, 1996. 816p.
- Stinson, Douglas R. Cryptography: Theory and Practice. New York: CRC Press, 1995. 448p.
- Artigos científicos sobre o assunto, disponíveis no portal da Capes