

**INSTITUTO FEDERAL**  
Paraíba

Campus  
João Pessoa

## **Curso Superior de Tecnologia em Sistemas para Internet**

### **Disciplina – Segurança de Dados**

Prof. Leandro Almeida ([leandro.almeida@ifpb.edu.br](mailto:leandro.almeida@ifpb.edu.br))

# Objetivos

---

- Obter uma visão geral sobre Segurança da Informação e proteção de dados usando mecanismos e protocolos adequados
  - Conhecer técnicas, aplicações, protocolos e equipamentos para segurança de dados
  - **Estudar criptografia (teoria e prática)**
  - Estudar protocolos e aplicações para segurança em redes
  - Avaliar técnicas e ferramentas de ataques e de proteção em redes de computadores

# Conteúdo

---

- Unidade 1 - Introdução à Segurança da Informação
- Unidade 2 - Autenticação, controle de acesso e funções hash
- Unidade 3 - Criptografia
- Unidade 4 - Certificados digitais
- Unidade 5 - Transport Security Layer
- Unidade 6 - Firewall
- Tópicos emergentes em segurança

# Metodologia

---

## Aulas expositivas e demonstrativas

- Slide
- Quadro

## Aulas práticas

- Ferramentas utilizadas por hacker e administradores

## Seminários

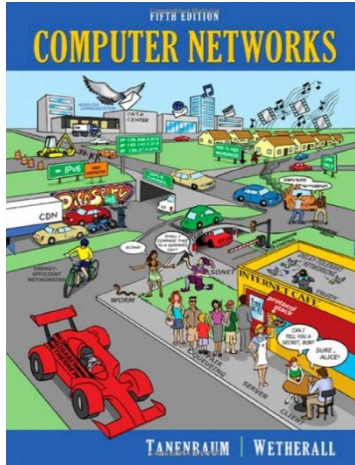
# Avaliações

---

- Duas provas (**P1**, **P2**)
- Apresentação de Seminário (**S**)
- Nota de presença em Laboratórios (**L**)
- Nota de presença em seminários dos colegas (**PS**)

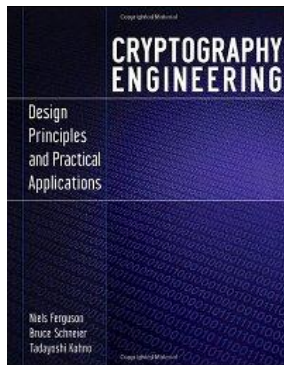
$$\text{Média} = 30\%S + 25\%P1 + 25\%P2 + 15\%L + 5\%PS$$

# Bibliografia

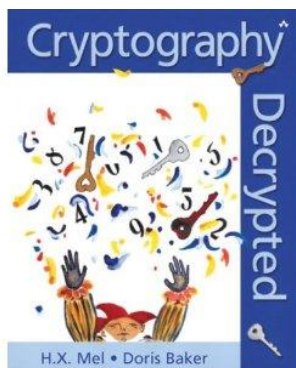


- Andrew S. Tanenbaum, David J. Wetherall. **Computer Networks (5th Edition)**. Prentice Hall, 2010  
(Capítulo 8)

# Bibliografia



- Niels Ferguson, Bruce Schneier, Tadayoshi Kohno. **Cryptography Engineering: Design Principles and Practical Applications.** Wiley, 2010



- H. X. Mel and Doris M. Baker. **Cryptography Decrypted.** Addison-Wesley, 2000.