Serviço Público Federal
Instituto Federal de Educação, Ciência e Tecnologia Sul-rio-grandense
Pró-Reitoria de Ensino
Campus Pelotas
Curso de Engenharia Elétrica

DISCIPLINA: Criptografia e Segurança de Dados	
Vigência: a partir de 2007/1	**Período Letivo:** Eletiva
Carga Horária Total: 45h	**Código:** EE.373
Ementa: Encriptação de chave pública e privada. Criptografia simétrica e assimétrica. Funções de hash. Assinaturas digitais. Geradores de números pseudo-aleatórios. Protocolos de encriptação. Medidas de complexidade computacional. Demanda computacional de algoritmos. Algoritmos criptográficos aplicados.	

Conteúdos

Unidade 1. Criptografia
- 1.1. Introdução
- 1.2. Encriptação de chave publica e privada
- 1.3. Criptografia simétrica e assimétrica
- 1.4. Funções de hash.
- 1.5. Assinaturas digitais
- 1.6. Geradores de números pseudo-aleatórios

Unidade 2. Implementação
- 2.1. Protocolos de encriptação
- 2.2. Medidas de complexidade computacional.
- 2.3. Demanda computacional de algoritmos.
- 2.4. Algoritmos criptográficos aplicados.

Bibliografia básica:

STALLINGS, William. **Criptografia e Segurança de Redes – Princípios e Práticas.** Prentice Hall.
BISHOP, Matthew. **Computer Security – Art and Science.** Addison and Wesley, 2002.
DHANJANI, Nitesh. **Hacking – Next Generation.** Oreilly, 2009.

Bibliografia complementar:

VACCA, John. **Computer and Information Security Handbook.** Elsevier Science.
BURNETT, Steven. **Criptography Decripted.** Addison Wesley.
IAN, Song Y. **Criptanalictics Attacks on RSA.** New York: Springer Verlag, 2007.
DAVIS, Chris. **Hacking Exposed Computer Forensics.** McGraw-Hill.
SNYDER, Charles. **Security Management.** Prentice Hall.