

Segurança Computacional

Luiz Carlos Zancanella, D.Sc.

Graduação em Sistemas de Informação

INE / UFSC - SC

Programa

- **Introdução a Criptografia,**
- **Criptografia simétrica,**
- **Criptografia assimétrica,**
- **Função Hash,**
- **Assinatura digital,**
- **Infra-estrutura de Chaves Públicas,**
- **Protocolos Criptográficos,**

Bibliografia

- Schneier, Bruce. Applied Cryptography: Protocols, Algorithms, and Source Code in C. 2nd Edition, New York: John Wiley & Sons, 1995. 784p.
- Stallings, William. Cryptography and Network Security: Principles and Practice. Prentice Hall, 1999. 569p.
- RSA Data Security, Inc. “Frequently Asked Questions about Today’s Cryptography”. 1998. <http://www.rsa.com>.
- Menezes, Alfred J., at all. A Handbook of Applied Cryptography. New York: CRC Press, 1996. 816p.
- Feghhi, Jalal, at all. Digital Certificates: Applied Internet Security. New York: Addison-Wesley, 1998. 453p.
- Stinson, Douglas R. Cryptography: Theory and Practice. New York: CRC Press, 1995. 448p.