Tópicos Especiais em Segurança da Informação

Flávio de Oliveira Silva

flavio@facom.ufu.br

Objetivos

- Conhecer os principais serviços relacionados com a segurança da informação e sua implementação através de técnicas de criptografia
- Conhecer e entender fundamentos de criptografia;
- Conhecer funcionamento de algoritmos simétricos e assimétricos
- Adquirir capacidade de escolher técnicas de criptografia conforme a necessidade
- Conhecer e implementar serviços de segurança utilizado a JCA (Java Cryptographic Architecture)

Conteúdo Programático

- Criptografia e Criptoanálise
- Algoritmos Simétricos
  - Técnicas clássicas
  - Block Ciphers (DES)
  - Advanced Encription Standards (AES)
  - Modos de Operação
- Java Cryptographic Extension
- Algoritmos Assimétricos
  - Conceitos e Aplicações
  - RSA
- Serviços de Segurança
- Message Autentication Codes (MAC)
- Algoritmos Hash
- Assinaturas Digitais
- Implementação Serviços de Segurança

Bibliografia

- STALLINGS, W. **Criptografia e segurança de redes : princípios e práticas**. 4 ed. São Paulo: Prentice Hall, 2008
- STALLINGS, W. **Cryptography and Network Security: Principles and Practice**. 4th ed. Upper Saddle River, NJ : Pearson, 2006.
- STALLIGNS, W. Network security essentials: applications and standards. 2nd ed. Upper Saddle River, NJ : Pearson, 2003.
- HOOK, D. **Beginning Cryptography with Java**. 1ed. 2005

Avaliação

- Teórica – 50 pontos
  - Duas avaliações
    - Sem consulta
- Prática – 50 pontos
  - Laboratório – 10 pontos
    - Participação no Laboratório (Presença + Atividade Prática)
    - Atividades realizadas em Laboratório enviadas por e-mail no dia de sua realização
  - Trabalhos
    - Final de Curso
    - Todos os trabalhos iguais (ou similares) serão desconsiderados

Sua opinião?

- Email
  - flavio@facom.ufu.br
  - Titulo = [TESI]Objetivos
- Questões
  - O que você espera da disciplina “Tópicos Especiais em Segurança da Informação”?
  - Qual sua opinião sobre o BSI/BCC?
  - Como você avalia sua dedicação aos estudos? Em que ela pode ser melhorada?
  - Nome completo
  - Matrícula
- Observação
  - Enviar da conta de e-mail mais utilizada
  - Enviar até 28/05/2013