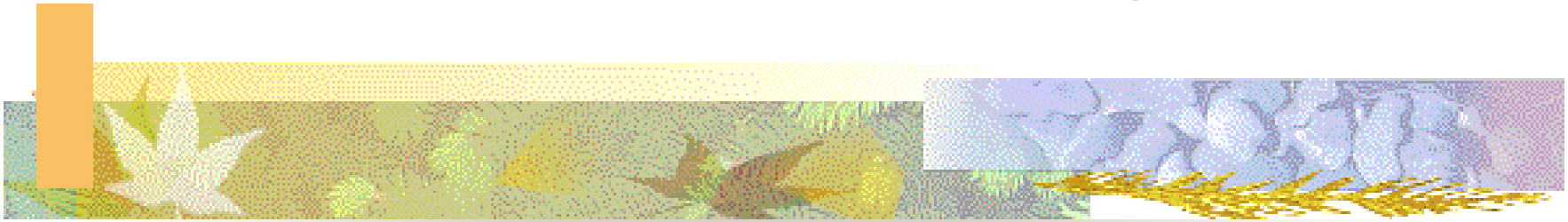
Introdução à Criptografia



Profa. Yeda

Aula 1 - Apresentação

Introdução à Criptografia

- Pré-requisitos
  - 2011: POO E CD
  - 2018: MD E ED
- Objetivo
  - Fornecer uma **visão** panorâmica das **técnicas criptográficas** atuais mais importantes para atender aos **requisitos** fundamentais da **segurança** da informação e comunicação.

Introdução à Criptografia

- Ementa
  - Introdução à criptografia.
  - Fundamentos matemáticos.
  - Algoritmos simétricos.
  - Algoritmos assimétricos.
  - Função resumo.
  - Assinatura digital.
  - Aplicações.

Introdução à Criptografia

- Horário de Aula
  - Terça – 08:00 às 11:46h
- Horário de Atendimento: agendado
- Material de aula disponível no Classroom.
  - Código da turma: dgawbf

Introdução à Criptografia

- Composição da Nota
  - P1 e P2: provas
    - Avaliações parciais substituem 1 questão da prova
  - At: média das atividades práticas

$$M = P1 * 0,4 + P2 * 0,4 + At * 0,2$$

  - Será aprovado se $M \geq 6,0$ e frequência $\geq 75\%$

Introdução à Criptografia

- Avaliação Complementar (SAC)
  - Requisito: $5{,}0 \leq M < 6{,}0$ e frequência $\geq 75\%$
  - Data: início do semestre seguinte
  - Prova incluindo todo o conteúdo.

$$MF = (M + AC)/2$$

- DATAS DAS PROVA
  - 31/10/2018 – 1ª avaliação
  - 19/12/2018 – 2ª avaliação

Bibliografia

- **Christof Paar e Jan Pelzl. Understanding Cryptography - A Textbook for Students and Practitioners. Springer, 2010.**
- A. Menezes, P. C. van Oorschot, S. Vanstone. **Handbook of Applied Cryptography**. CRC Press. 1997. **(2)**
- D. R. Stinson. **Cryptography - Theory and Practice**. CRC Press. 2a. Edição. 2006.**(2)**
- B. Schneier. Applied Cryptography. John Wiley & Sons. 2ª Edição. 1996. **(2)**
- W. Stallings. Criptografia e Segurança de Redes. Prentice-Hall. 2010. **(12)**
- D. Challener; K. Yoder; R. Catherman. A Practical Guide to Trusted Computing. Prentice-Hall. 2008. **(1)**
- P. C. da Silva; L. G. C. da Silva; I. J. de S. Aquino Junior. Certificação Digital - Conceitos e Aplicações. Ciência Moderna. 2008. **(6)**
- N. S. Yanofsky, M. A. Mannucci. Quantum computing for computer scientists. Cambridge: Cambridge University Press, 2008. xvi, 384 p. **(13)**