DADOS DE IDENTIFICAÇÃO DO COMPONENTE CURRICULAR		
AL2159 TÓPICOS DE SEGURANÇA EM REDES DE COMUNICAÇÃO		
Carga horária: 60h	Créditos teóricos: 4	Créditos práticos: 0
Pré-requisito(s): Algoritmos e Programação (essencial), Redes de Comunicação (essencial)		
Semestre recomendado: 6° Semestre		

OBJETIVOS

Especificar, projetar e implementar redes seguras de computadores e comunicação de acordo com as normas especificadas pela IEEE.

EMENTA

Conceitos básicos de Redes de Computadores e Comunicação. Introdução aos Sistemas Criptográficos. Ataque de Segurança, Serviço de Segurança e Mecanismos de Segurança. Técnicas Clássicas de Criptografia. Algoritmos de Cifras Simétricas. Técnicas de Substituição. Técnicas de Transposição, Esteganografia, Funções de Resumo (Hash). Algoritmos de Cifras Assimétricas. Assinaturas Digitais.

REFERÊNCIAS BÁSICAS (LEITURAS OBRIGATÓRIAS)

STALLINGS, William. **Criptografia e Segurança de Redes**. Pearsons, 2010.

STALLINGS, William. **Redes e Sistemas de Comunicação de Dados**. Elsevier, 2005.

FOROUZAN, Behrouz A. **Comunicação de Dados e Redes de Computadores**. McGraw-Hill, 2008.

REFERÊNCIAS COMPLEMENTARES

NAKAMURA, E. T., GEUS. P. L. **Segurança de Redes em Ambientes cooperativos**. Ed. Novatec. 2007.

COLLIER COUTINHO, Severino . **Números Inteiros e Criptografia RSA**. IMPA, 2014.

TANENBAUM, Andrew S. **Redes de Computadores**. Campus, 2003.

TERADA, Routo **Segurança de Dados - Criptografia em Rede de Computador** Blucher, 2008.

KATZ, Jonathan; LINDELL, Yeahuda **Introduction to Modern Cryptography** Chapman & Hall, 2007.