DISCIPLINA: Criptografia e Segurança de Dados	
Vigência: a partir de 2021/2	**Período letivo:** Eletiva
Carga horária total: 45h	**Código:** EE.373
Ementa: Apresentar ao aluno a teoria, prática e os princípios para o desenvolvimento de sistemas que visem a segurança de dados e das informações que trafegam em uma rede de computadores.	

Conteúdos

UNIDADE I - Cifras clássicas

1.1 Introdução
1.2 Requisitos de segurança de rede
1.3 Cifras clássicas

UNIDADE II - Cifras simétricas

2.1 Algoritmo DES
2.2 Teoria de Corpos Finitos
2.3 Algoritmo AES
2.4 Outras cifras de bloco
2.5 Confidencialidade usando cifras simétricas

UNIDADE III - Cifras assimétricas

3.1 Teoria dos números
3.2 Criptografia de chave pública e algoritmo RSA
3.3 Gerenciamento de chaves e outros criptossistemas de chave pública
3.4 Acordo de chaves Diffie-Hellmann
3.5 Autenticação de mensagens e funções de Hash
3.6 Assinaturas digitais e protocolos de autenticação

UNIDADE IV - Aplicações de criptografia

4.1 Kerberos e X-509
4.2 PGP e S-MIME

Bibliografia básica

STALLINGS, William. **Criptografia e Segurança de Redes – Princípios e Práticas.** - 4 ed. Prentice Hall.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício de. **Segurança de redes em ambientes cooperativos.** São Paulo, SP: Novatec, 2007. 483 p. ISBN 9788575221365.

DHANJANI, Nitesh; HARDIN, Brett. **Hacking:** the next generation. Sebastopol (ca): Oreilly, 2009. 279 p. : il. p.

GOODRICH, Michael T.; LISBÔA, Maria Lúcia Blanck (Tradutora). **Introdução à segurança de computadores.** Porto Alegre, RS: Bookman, 2013. 550 p. ISBN 9788540701922.

Bibliografia complementar

BISHOP, Matthew. **Computer Security – Art and Science.** Addison and Wesley, 2002.

DHANJANI, Nitesh; RIOS, Billy; HARDIN, Brett (Aut.). **Hacking:** a próxima geração. Rio de Janeiro, RJ: Alta Books, 2011. xiii, 273 p. ISBN 9788576085331.

MITNICK, Kevin David; SIMON, William L. **A arte de invadir:** as verdadeiras histórias por trás das ações de hackers, intrusos e criminosos eletrônicos. São Paulo: Pearson, 2006. xv, 236 p. ISBN 9798576050550

YAN, Song Y. **Cryptanalytic attacks on RSA.** New York: Springer, c2008. xx, 254 p. ISBN 9780387487410

MEL, H. X; BAKER, Doris M. **Cryptography decrypted.** Boston: Addison-Wesley, c2001. xx, 352 p. ISBN 9780201616477

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. **Hackers expostos:** segredos e soluções para a segurança de redes. 4. ed. Rio de Janeiro, RJ: Campus, 2003. 784p. p.