Ministério da Educação
UNIVERSIDADE FEDERAL DO PARANÁ
Setor de Ciências Exatas
Coordenação do Curso de Bacharelado em Ciência da Computação ou
Departamento de Informática

Ficha 2 (variável)

Disciplina: Criptografia						Código: CI1017
Natureza: (X) Obrigatória ( ) Optativa	(X) Semestral ( ) Anual ( ) Modular					
Pré-requisito:	Co-requisito:	Modalidade: ( ) Presencial (X) Totalmente EaD ( )..... % EaD*				
CH Total: 60 **CH semanal: 04**	Padrão (PD): 40	Laboratório (LB): 0	Campo (CP): 0	Estágio (ES): 0	Orientada (OR): 0	Prática Específica (PE): 20

EMENTA (Unidade Didática)

Algoritmos criptográficos.

PROGRAMA (itens de cada unidade didática)

- Introdução a criptografia
- Criptografia simétrica clássica – substituição, transposição, rotor
- Criptografia simétrica moderna – DES, 3DES, AES
- Criptografia assimétrica – RSA, ECC
- Assinaturas digitais
- Cifras de fluxo – RC4
- Acordo de chaves
- Gerenciamento de chaves

OBJETIVO GERAL

O aluno deve ter uma compreensão histórica da importância da criptografia.
Deve conhecer os detalhes dos algoritmos criptográficos clássicos e modernos.
Deve conhecer os principais ataques e formas de quebrar os algoritmos criptográficos.

OBJETIVO ESPECÍFICO

O aluno deve compreender a história e a evolução da criptografia, desde os algoritmos clássicos até os algoritmos modernos. Deve compreender as formas tradicionais de ataques aos algoritmos criptográficos, incluindo força bruta, análise de frequência. Deve conhecer assinatura digitais através de algoritmos criptográficos, gerenciamento de chaves de criptografia e acordo de chaves.

PROCEDIMENTOS DIDÁTICOS

Aulas expositivas.

FORMAS DE AVALIAÇÃO

2 trabalhos + 1 prova

BIBLIOGRAFIA BÁSICA (mínimo 03 títulos)

- *Criptografia e segurança de redes: princípios e práticas. William Stallings., Pearson Prentice Hall, 2008.*

- *Introduçao a criptografia computacional. Claudio Leonardo Lucchesi. Ed. da UNICAMP, 1986.*

- *Foundations of Cryptography: Volume 1, Basic Tools*. Goldreich, Oded. Cambridge University Press. 2003.

http://www.inf.ufpr.br/albini/tutorial_cripto/index.html

BIBLIOGRAFIA COMPLEMENTAR (mínimo 05 títulos)

- *Elliptic Curves in Cryptography. Blake, Ian F., Smart, Nigel P., Seroussi, G. Cambridge University Press. 1999.*

- *Computer Security and Cryptography. Konheim, Alan G. Wiley-Interscience. 2007.*

- *Identity-based Cryptography. Neven, Gregory, Joye, Marc. IOS Press. 2009*

- *Practical Cryptography. Bruce Schneier. Wiley, 2003*

- *Applied Cryptography. Bruce Schneie. Wiley 1996*

http://www.inf.ufsc.br/~bosco.sobral/ensino/ine5630/material-cripto-seg/Introducao-Criptografia.pdf

http://www.mat.ufpb.br/bienalsbm/arquivos/Oficinas/PedroMalagutti-TemasInterdisciplinares/Aprendendo_Criptologia_de_Forma_Divertida_Final.pdf

https://www.mathematik.uni-kl.de/~ederc/download/Cryptography.pdf

https://crypto.stanford.edu/~dabo/cryptobook/draft_0_2.pdf

Professor da Disciplina: Luiz Carlos Pessoa Albini

Assinatura: _____

Chefe de Departamento ou Unidade equivalente: Fabiano Silva

Assinatura: _____

**OBS: ao assinalar a opção % EAD, indicar a carga horária que será à distância.*