MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PARANÁ
SETOR DE CIÊNCIAS EXATAS

Departamento de Informática

Ficha 1 (permanente)

Disciplina: Criptografia							Código: CI1017
Natureza: ( ) Obrigatória (x) Optativa	(x) Semestral ( ) Anual ( ) Modular						
Pré-requisito: CI1055 / CI1068 / CI1003 / CMA111 / CM304 / CI1056 / CI1210 / CI1001 / CMA211 / CM303 / CI1057 / CI1212 / CI1002 / CI1237 / CE009 /	Co-requisito:	Modalidade: (x) Presencial ( ) Totalmente EAD ( ) CH em EAD: _____					
CH Total: 60 CH Semanal: 4	Padrão (PD): 40	Laboratório (LB): 20	Campo (CP): 0	Estágio (ES): 0	Orientada (OR): 0	Prática Específica (PE): 0	Estágio de Formação Pedagógica (EFP):0

EMENTA

Algoritmos criptográficos.

**OBS (1): ao assinalar a opção CH em EAD, indicar a carga horária que será à distância.*

Art. 9º da Resolução 30/90 – CEPE

Padrão (PD): conjunto de estudos e atividades desenvolvidos fundamentalmente nos espaços de aprendizagem considerados padrão para as modalidades de ensino presencial e de educação à distância (EAD).

Laboratório (LB): conjunto de estudos e atividades desenvolvidos fundamentalmente em espaços de aprendizagem estabelecidos com infraestrutura especializada, tais como laboratórios, oficinas e estúdios.

Campo (CP): conjunto de estudos e atividades desenvolvidos fundamentalmente mediante atividades de campo.

Estágio (ES): conjunto de estudos e atividades desenvolvidos fundamentalmente em ambientes de trabalho mediante estágios regulados pela Lei nº 11.778, de 25 desetembro de 2008.

Orientada (OR): conjunto de estudos e atividades direcionados à vivência na atuaçãoacadêmica e/ou profissional, em seus mais amplos aspectos, desenvolvidos em espaços educacionais internos e/ou externos à UFPR, com a participação direta de docente responsável.

Práticas Específicas (PE): conjunto de atividades de natureza prática, desenvolvidas em ambientes que apresentem restrições ao quantitativo de alunos por docente e que exijam controle rigoroso envolvendo questões de segurança, dignidade, privacidade e sigilo e/ou atenção do docente individualizada ou a pequenos grupos para desenvolvimento do processo de ensino-aprendizagem, com a participação direta do docente responsável.

Estágio de Formação Pedagógica (EFP): conjunto de estudos e atividades desenvolvidas fundamentalmente no âmbito da educação básica, sob a forma de "práticas de docência" e "práticas pedagógicas de organização do trabalho escolar", envolvendo a orientação direta docente em ações que vão desde a intermediação no acordo de colaboração entre a UFPR e os estabelecimentos de ensino, até o acompanhamento sistemático e processual do planejamento, da execução e da avaliação das atividades desenvolvidas pelos licenciandos, o que requer o contato contínuo e presencial do professor nos diferentes campos de estágio e consequentemente a limitação de alunos por turma.

BIBLIOGRAFIA BÁSICA (mínimo 03 títulos)

[1] Criptografia e segurança de redes: princípios e práticas. William Stallings., Pearson Prentice Hall, 2008.

[2]Introduçao a criptografia computacional. Claudio Leonardo Lucchesi. Ed. da UNICAMP, 1986.

[3] Foundations of Cryptography: Volume 1, Basic Tools. Goldreich, Oded. Cambridge University Press. 2003.

BIBLIOGRAFIA COMPLEMENTAR (mínimo 05 títulos)

[4] Elliptic Curves in Cryptography. Blake, Ian F., Smart, Nigel P., Seroussi, G. Cambridge University Press. 1999.

[5] Computer Security and Cryptography. Konheim, Alan G. Wiley-Interscience. 2007.

[6] Identity-based Cryptography. Neven, Gregory, Joye, Marc. IOS Press. 2009

[7] Practical Cryptography. Bruce Schneier. Wiley, 2003

[8] Applied Cryptography. Bruce Schneie. Wiley 1996