UNIVERSIDADE FEDERAL DE UBERLÂNDIA
FACULDADE DE COMPUTAÇÃO
COLEGIADO DO CURSO DE CIÊNCIA DA COMPUTAÇÃO

FICHA DE DISCIPLINA

DISCIPLINA: SEGURANÇA DA INFORMAÇÃO

CÓDIGO: GBC083		**UNIDADE ACADÊMICA:** FACULDADE DE COMPUTAÇÃO		
PERÍODO/SÉRIE: - 8º. Período		**CH TOTAL TEÓRICA:**	**CH TOTAL PRÁTICA:**	**CH TOTAL:**
OBRIGATÓRIA: (X)	**OPTATIVA:** ( )	60	00	60
NÚCLEO DE FORMAÇÃO: Tecnológica / Profissional				
PRÉ-REQUISITOS: NÃO HÁ		**CÓ-REQUISITOS: NÃO HÁ**		

OBJETIVOS

Conhecer os principais serviços relacionados com a segurança da informação e sua implementação através de técnicas de criptografia.
Conhecer e entender fundamentos de criptografia.
Conhecer funcionamento de algoritmos simétricos e assimétricos.
Adquirir capacidade de escolher técnicas de criptografia conforme a necessidade
Conhecer e implementar serviços de segurança utilizado a JCA (Java Cryptographic Architecture)

EMENTA

Breve histórico da criptografia clássica e moderna. Conceituação de sistemas simétricos e assimétricos. Principais algoritmos simétricos e assimétricos de ciframento. Principais algoritmos para "hashing" criptográfico. Principais algoritmos para assinaturas digitais. Protocolos para negociação de chaves. Protocolos para autenticação em sistemas distribuídos. Protocolos IPSec, SSL e TLS. Introdução à Segurança da informação, Planejamento de Contingência e Continuidade de Negócios, Políticas e Normas em Segurança. Certificação de sistemas e de software. Segurança em Aplicações, Segurança de Operações, Segurança de Redes e Telecomunicações.

Fl. Nº 209

DESCRIÇÃO DO PROGRAMA

1. Conceitos Segurança
2. Tipos de Ataques
3. Serviços e Mecanismos de Segurança
4. Criptografia e Criptoanálise
5. Algoritmos Simétricos
   - 5.1. Técnicas clássicas
   - 5.2. Block Ciphers (DES)
   - 5.3. Advanced Encription Standards (AES)
   - 5.4. Modos de Operação
6. Java Cryptographic Extension (Cifradores Simétricos
7. Algoritmos Assimétricos
   - 7.1. Conceitos e Aplicações
   - 7.2. RSA
8. Message Autentication Codes (MAC)
9. Algoritmos Hash
10. Assinaturas Digitais
11. Public Key Infraestructure
    - 11.1. Certificados Digitais e Certificados X.509
12. Segurança Camada Aplicação da Arquitetura TCP/IP
    - 12.1. TLS (Transport Layer Security)
13. Implementação Serviços de Segurança

BIBLIOGRAFIA

Básica

Stallings, William. Criptografia e segurança de redes : princípios e práticas / William Stallings ; tradução: Daniel Vieira ; revisão técnica: Ákio Nogueira Barbosa, Marcelo Succi de Jesus Ferreira. São Paulo : Prentice Hall, 2008.

Stallings, William. Network security essentials : apllications and standards / William Stallings. 2nd ed, Upper Saddle River : Prentice Hall, 2003.

Complementar

Brands, Stefan A. Rethinking public key infrastructures and digital certificates : building in privacy. Cambridge, Mass. : MIT Press, 2000.

Burnett, Steve. RSA Security's official guide to cryptography. New York : Osborne/McGraw-Hill, 2001.

Ford, Warwick. Secure electronic commerce : building the infrastructure for digital signatures and encryption . 2nd ed. Upper Saddle River, NJ : Prentice Hall PTR, 2001.

APROVAÇÃO

/ /

Carimbo e assinatura do Coordenador do curso

Universidade Federal de Uberlândia
Prof. Ilmério Reis da Silva
Coordenador do Curso de Ciência da Computação
Portaria R nº 713/08

Carimbo e assinatura do Diretor

Universidade Federal de Uberlândia
Prof. Junior Barbar
Diretor da Faculdade de Computação
Portaria R nº 672/07