



UNIVERSIDADE FEDERAL DE UBERLÂNDIA
 FACULDADE DE COMPUTAÇÃO
 COLEGIADO DO CURSO DE SISTEMAS DE INFORMAÇÃO

FICHA DE DISCIPLINA

DISCIPLINA: TÓPICOS ESPECIAIS DE SEGURANÇA DA INFORMAÇÃO

CÓDIGO: GSI078		UNIDADE ACADÊMICA: FACULDADE DE COMPUTAÇÃO		
PERÍODO/SÉRIE: 7º OU 8º		CH TOTAL TEÓRICA:	CH TOTAL PRÁTICA:	CH TOTAL:
OBRIGATÓRIA: ()	OPTATIVA: (X)	60	00	60
OBS:				
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
- Utilizar na prática algoritmos simétricos e assimétricos
- Conhecer e implementar serviços de segurança utilizado a JCE (Java Cryptographic Extension)

EMENTA

Segurança e Criptografia – Conceitos Básicos. JCE (Java Cryptographic Extension) Aplicação e Uso. Algoritmos Simétricos. Algoritmos Assimétricos. Message Authentication Codes. Funções Hash. Certificados X509.

W JKO



DESCRIÇÃO DO PROGRAMA

1. Introdução
2. Serviços de Segurança
3. Algoritmos Simétricos
4. Algoritmos Assimétricos
5. Message Authentication Codes (MAC)
6. Funções Hash
7. Java Cryptographic Extension
 - 7.1. Conceitos e Provedores
 - 7.2. Engines
 - 7.3. Cifradores
 - 7.4. Representação de Chaves
 - 7.5. Geração de Chaves
 - 7.6. Certificados X509 – Armazenamento e Representação
8. Implantação Serviços de Segurança utilizando JCA

BIBLIOGRAFIA

BÁSICA

Weiss, James. Java Cryptography Extensions: Practical Guide for Programmers (The Practical Guides). Morgan Kaufmann, 2004

Stallings, W. Cryptography and Network Security: Principles and Practice. Prentice-Hall, 2002.

COMPLEMENTAR

Ferguson, N.; Schneier, B. Practical Cryptography. Wiley Publishing, 2003.

Knudsen, Jonathan B. Java Cryptography. O'Reilly, 1998

APROVAÇÃO

08/11/2011

Carimbo e assinatura do Coordenador do curso

Universidade Federal de Uberlândia
Prof. Dr. Daniel Gomes Mesquita

Coordenador do Curso de S.stemas de Informação

Portaria R Nº. 1257/10

08/11/2011

Carimbo e assinatura do Diretor da
Unidade Acadêmica

Universidade Federal de Uberlândia

Prof. Ilmério Reis da Silva
Diretor da Faculdade de Computação

Portaria R Nº. 757/11