UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FICHA DE COMPONENTE CURRICULAR

CÓDIGO: GBC083	**COMPONENTE CURRICULAR:** SEGURANÇA DA INFORMAÇÃO	
UNIDADE ACADÊMICA OFERTANTE: FACULDADE DE COMPUTAÇÃO		**SIGLA:** FACOM
CH TOTAL TEÓRICA: 60 horas	**CH TOTAL PRÁTICA:** 00 horas	**CH TOTAL:** 60 horas

1. OBJETIVOS

- Aplicar os principais serviços relacionados com a segurança da informação e sua implementação através de técnicas de criptografia.
- Aplicar os fundamentos de criptografia.
- Implementar algoritmos simétricos e assimétricos.
- Selecionar técnicas de criptografia conforme a necessidade.
- Implementar serviços de segurança utilizado a JCA (Java Cryptographic Architecture).

2. 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.

3. PROGRAMA

1. Conceitos Segurança
2. Tipos de Ataques
3. Serviços e Mecanismos de Segurança
4. Criptografia e Criptoanálise
5. Algoritmos Simétricos
    - Técnicas clássicas
    - Block Ciphers (DES)

- Advanced Encription Standards (AES)
- Modos de Operação

6. Java Cryptographic Extension (Cifradores Simétricos)
7. Algoritmos Assimétricos
   - Conceitos e Aplicações
   - RSA
8. Message Autentication Codes (MAC)
9. Algoritmos Hash
10. Assinaturas Digitais
11. Public Key Infrastructure
    - Certificados Digitais e Certificados X.509
12. Segurança Camada Aplicação da Arquitetura TCP/IP
    - TLS (Transport Layer Security)
13. Implementação Serviços de Segurança

4. BIBLIOGRAFIA BÁSICA

1. STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson, c2015.

2. MORENO, Edward David. **Criptografia em software e hardware**. São Paulo: Novatec, c2005.

3. BUCHMANN, Johannes A. **Introdução à criptografia**. São Paulo: Berkeley Brasil, 2002.

5. BIBLIOGRAFIA COMPLEMENTAR

1. LUCCHESI, Claudio Leonardo. **Introdução a criptografia computacional**. Campinas: Ed. da UNICAMP, 1986.

2. STALLINGS, William. **Network security essentials**: apllications and standards. 2nd ed. Upper Saddle River: Prentice Hall, c2003.

3. BRANDS, Stefan A. **Rethinking public key infrastructures and digital certificates**: building in privacy. Cambridge: MIT Press, c2000.

4. BURNETT, Steve. **RSA Security's official guide to cryptography**. New York: Osborne: McGraw-Hill, 2001.

5. FORD, Warwick. **Secure electronic commerce**: building the infrastructure for digital signatures and encryption. 2nd ed. Upper Saddle River: Prentice Hall PTR, c2001.

6. APROVAÇÃO

Maria Adriana Vidigal de Lima
Coordenadora do Curso de Ciência da Computação

Maurício Cunha Escarpinati
Diretor da Faculdade de Computação

Documento assinado eletronicamente por **Maria Adriana Vidigal de Lima**, **Coordenador(a)**, em 26/01/2024, às 15:18, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Mauricio Cunha Escarpinati**, **Diretor(a)**, em 19/02/2024, às 11:33, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **5129220** e o código CRC **9BD84EB9**.

Referência: Processo nº 23117.053855/2023-26 SEI nº 5129220