UNIVERSIDADE FEDERAL DE UBERLÂNDIA

FICHA DE COMPONENTE CURRICULAR

CÓDIGO: GBC235	**COMPONENTE CURRICULAR:** TÓPICOS ESPECIAIS DE SEGURANÇA DA INFORMAÇÃO	
UNIDADE ACADÊMICA OFERTANTE: FACULDADE DE COMPUTAÇÃO		**SIGLA:** FACOM
CH TOTAL TEÓRICA: 60 horas	**CH TOTAL PRÁTICA:** 0 horas	**CH TOTAL:** 60 horas

1. OBJETIVOS

- Conhecer os principais serviços relacionados com a segurança da informação e sua implentação através de técnicas de criptografia
- Utilizar na prática algoritmos simétricos e assimétricos
- Conhecer e implementar serviços de segurança utilizado a JCE (Java Cryptographic Extension)

2. EMENTA

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

3. 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. Implentação Serviços de Segurança utilizando JCA

4. BIBLIOGRAFIA BÁSICA

1. STALLINGS, William. **Criptografia e segurança de redes**: princípios e práticas. 6. ed. São Paulo: Pearson, 2015.

2. PAAR, Christof; PELZL, Jan. **Understanding cryptography**: a textbook for students and practitioners. New York: Springer, c2010.

3. MORAES, Alexandre Fernandes de. **Segurança em redes**: fundamentos. São Paulo: Erica, 2010. *E-book*. Disponível em: https://www.sistemas.ufu.br/biblioteca-gateway/minhabiblioteca/9788536522081. Acesso em: 26 set. 2023.

5. BIBLIOGRAFIA COMPLEMENTAR

1. STALLINGS, W. **Cryptography and network security**: principles and practice. Upper Saddle River: Prentice Hall, 2006.

2. MORENO, Edward David. **Criptografia em software e hardware**. São Paulo: Novatec, 2005.

3. STINSON, Douglas R. **Cryptography**: theory and practice. 3rd ed. Boca Raton: Chapman & Hall/CRC Press, 2006.

4. BALDONI, M. Welleda. **Elementary number theory, cryptography, and codes**. Berlin: Springer, c2009.

5. MCCLURE, Stuart. **Hackers expostos**: segredos e soluções para a segurança de redes. Porto Alegre: Bookman, 2014. *E-book*. Disponível em: https://www.sistemas.ufu.br/biblioteca-gateway/minhabiblioteca/9788582601426. Acesso em 26 set. 2023.

6. APROVAÇÃO

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

Mauricio Cunha Escarpinati
Diretor da Faculdade de Computação

Documento assinado eletronicamente por **Maria Adriana Vidigal de Lima**, **Coordenador(a)**, em 26/01/2024, às 15:52, 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 **5134901** e o código CRC **630FC98C**.