



UNIVERSIDADE FEDERAL DE UBERLÂNDIA



## FICHA DE COMPONENTE CURRICULAR

<b>CÓDIGO:</b> GSI078	<b>COMPONENTE CURRICULAR:</b> TÓPICOS ESPECIAIS DE SEGURANÇA DA INFORMAÇÃO	
<b>UNIDADE ACADÊMICA OFERTANTE:</b> FACULDADE DE COMPUTAÇÃO		<b>SIGLA:</b> FACOM
<b>CH TOTAL TEÓRICA:</b> 60 horas	<b>CH TOTAL PRÁTICA:</b> 00 horas	<b>CH TOTAL:</b> 60 horas

1. **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 utilizando a JCE (*Java CryptographicExtension*)

2. **EMENTA**

Segurança e criptografia – conceitos básicos. JCE (*Java Cryptographic Extension*) aplicação e uso. Algoritmos 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. Implementação de serviços de segurança utilizando JCA

#### 4. BIBLIOGRAFIA BÁSICA

STALLINGS, W. **Criptografia e segurança de redes**: princípios e práticas. 4. ed. São Paulo: Prentice-Hall, c2008.

WEISS, J. **Java cryptography extensions**: practical guide for programmers. San Francisco: Morgan Kaufmann, 2004.

#### 5. BIBLIOGRAFIA COMPLEMENTAR

FERGUSON, N.; SCHNEIER, B. **Practical cryptography**. Indianapolis: Wiley Publishing, 2003.

KNUDSEN, J. **Java cryptography**. Sebastopol: O'Reilly, 1998.

#### 6. APROVAÇÃO

Prof. Dr. Jefferson Rodrigo de Souza  
Coordenador do Curso de Sistemas de Informação

Prof. Dr. Mauricio Cunha Escarpinati  
Diretor da Faculdade de Computação



Documento assinado eletronicamente por **Jefferson Rodrigo de Souza, Presidente**, em 21/12/2021, às 13:44, 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 01/02/2022, às 16:00, 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](https://www.sei.ufu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0), informando o código verificador **3211679** e o código CRC **431D567D**.