



**Ministério da Educação**  
**Universidade Tecnológica Federal do Paraná**  
**Câmpus Curitiba**



**Informações da disciplina**

| <b>Código Ofertado</b> | <b>Disciplina/Unidade Curricular</b> | <b>Modo de Avaliação</b>   | <b>Modalidade da disciplina</b> | <b>Oferta</b> |
|------------------------|--------------------------------------|----------------------------|---------------------------------|---------------|
| CSA44                  | Introdução À Criptografia            | Nota/Conceito E Frequência | Presencial                      | Semestral     |

| <b>Carga Horária</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |           |            |            |             |              |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|------------|------------|-------------|--------------|
| <b>AT</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | <b>AP</b> | <b>APS</b> | <b>ANP</b> | <b>APCC</b> | <b>Total</b> |
| 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | 4         | 4          | 0          | 0           | 60           |
| <ul style="list-style-type: none"> <li>• AT: Atividades Teóricas (aulas semanais).</li> <li>• AP: Atividades Práticas (aulas semanais).</li> <li>• ANP: Atividades não presenciais (horas no período).</li> <li>• APS: Atividades Práticas Supervisionadas (aulas no período).</li> <li>• APCC: Atividades Práticas como Componente Curricular (aulas no período, esta carga horária está incluída em AP e AT).</li> <li>• Total: carga horária total da disciplina em horas.</li> </ul> |           |            |            |             |              |

| <b>Objetivo</b>                                                                                                                                                           |                           |                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|--------------------------------------------------------|
| Proporcionar aos alunos conhecimentos sobre os fundamentos, algoritmos e aplicações da criptografia moderna.                                                              |                           |                                                        |
| <b>Ementa</b>                                                                                                                                                             |                           |                                                        |
| Introdução à Criptografia. Cifras de Fluxo. Cifras de Bloco. Criptografia com Sistemas de Chave Pública. Assinaturas Digitais. Resumos Criptográficos. Tópicos Avançados. |                           |                                                        |
| <b>Conteúdo Programático</b>                                                                                                                                              |                           |                                                        |
| <b>Ordem</b>                                                                                                                                                              | <b>Ementa</b>             | <b>Conteúdo</b>                                        |
| 1                                                                                                                                                                         | Introdução à Criptografia | História da criptografia. Importância da Criptografia. |
| 2                                                                                                                                                                         | Cifras de Fluxo           | Exemplos de cifras de fluxo. Vantagens e desvantagens. |
| 3                                                                                                                                                                         | Cifras de Bloco           | AES. DES.                                              |
| 4                                                                                                                                                                         | Assinaturas digitais      | Conceitos e algoritmos.                                |
| 5                                                                                                                                                                         | Resumos Criptográficos    | Hash (motivação, exemplos e aplicações).               |
| 6                                                                                                                                                                         | Tópicos avançados         | Estabelecimento de chaves. Criptografia Quântica.      |

| Bibliografia Básica                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------|
| PAAR, Cristof e PELZL, Jan. <b>Understanding Cryptography - A Textbook for Students and Practitioners</b> , Springer, 2010.        |
| CORMEN, Thomas H. et al. <b>Algoritmos: teoria e prática</b> . Rio de Janeiro, RJ: Elsevier, 2012. xvi, 926 p. ISBN 9788535236996. |
| STINTON, Douglas R. <b>Cryptography - Theory and Practice</b> . Chapman & Hall/CRC, 2005.                                          |

| Bibliografia Complementar                                                                                                                   |
|---------------------------------------------------------------------------------------------------------------------------------------------|
| TARDOS, E.. <b>Algorithm design</b> . Pearson Addison Wesley, 2005                                                                          |
| DASGUPTA, Sanjoy; PAPADIMITRIOU, Christos H.; VAZIRANI, Umesh. <b>Algoritmos</b> . São Paulo: McGraw-Hill, 2009. 320 p. ISBN 9788577260324. |
| SINGH, Simon. <b>The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography</b> . Anchor, 2000.                       |
| KATZ, J.; LINDELL, Y. <b>Introduction to Modern Cryptography</b> . Chapman & Hall/CRC, 2007.                                                |
| MAO, Wenbo. <b>Modern Cryptography - Theory and practice</b> . Pearson Education, 2004.                                                     |

| # | Resumo da Alteração     | Edição                                  | Data       | Aprovação                     | Data       |
|---|-------------------------|-----------------------------------------|------------|-------------------------------|------------|
| 1 | Plano de ensino criado. | Murilo Vicente<br>Goncalves Da<br>Silva | 29/03/2017 | Leonelo Dell<br>Anhol Almeida | 05/04/2017 |