

CE100 Algorithms and Programming II

Week-13 (Symmetric and Asymmetric Encryption)

Spring Semester, 2021-2022

Download [DOC](#), [SLIDE](#), [PPTX](#)

`<iframe width=700, height=500 frameBorder=0 src="../../ce100-week-13-symenc.md_slide.html"> </iframe>`

Symmetric and Asymmetric Encryption

Outline

- Symmetric Encryption Algorithms
- AES
- <https://formaestudio.com/portfolio/aes-animation/>
- DES
- <http://desalgorithm.yolasite.com/>
- TDES
- https://en.wikipedia.org/wiki/Triple_DES

- Symmetric Encryption Modes
- https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation
 - ECB
 - CBC
 - Asymmetric Encryption
 - Key Pairs (Public-Private Key Pairs)
 - Signature Generation and Validation

References

TODO