CE100 Algorithms and Programming II

Symmetric and Asymmetric Encryption

Author: Asst. Prof. Dr. Uğur CORUH

## CE100 Algorithms and Programming II

## Week-13 (Symmetric and Asymmetric Encryption)

#### Spring Semester, 2021-2022

Download [DOC](ce100-week-13-symenc.tr.md_doc.pdf), [SLIDE](ce100-week-13-symenc.tr.md_slide.pdf), [PPTX](ce100-week-13-symenc.tr.md_slide.pptx)

## 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