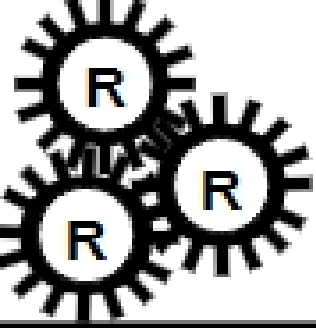


---

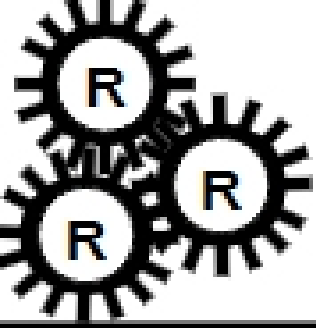
# Encryption

## A Brief Overview



# Encryption

- Encryption:
  - Definition: mechanisms to disguise the message so that if the intermission is intercepted/diverted, the content of the message will not be understood.
  - Impact: foundational building block to security-based computing



# Terminology

- Scenario:
  - S wants to send the message T to R, where an outsider, O, wants the message and tries to access it.
  - S: Sender
  - R: Receiver
  - T: Transmission Medium
  - O: Interceptor or Intruder.
- 4 ways O might try to access message.
  - Block it: prevent T from reaching R (availability)
  - Intercept it: read or listen to message (secrecy)
  - Modify it: obtaining message and changing it
  - Fabricate: generate an authentic-looking message to be delivered to R appearing to come from S