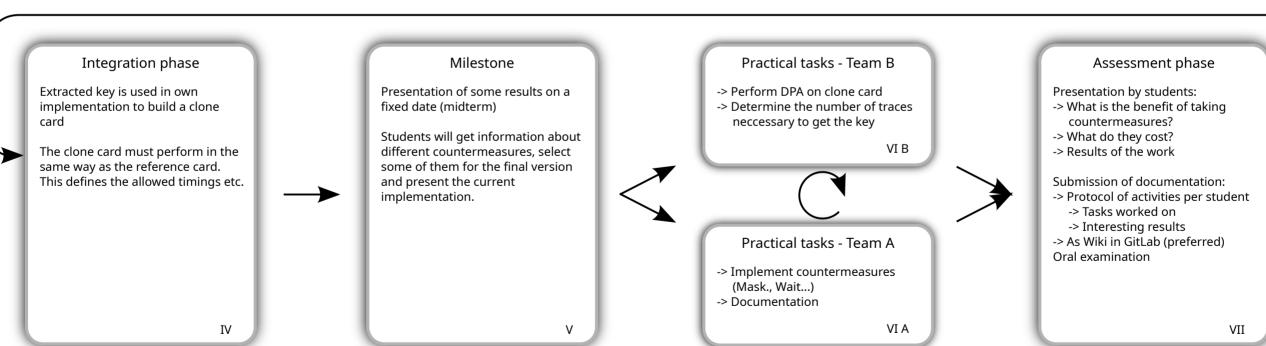


## SmartCard Lab



## First introduction Introduction to DPA Practical tasks - Team A Starting Situation Answers the following questions: Introduction to the differential -> Perform DPA What you get: -> Reference implementation of a What is the goal? power analysis: -> Extract key PayTV card -> Improve the security of a How does the AES algorithm work? -> Documentation PayTV card. How is the AES attacked and why? -> PCs with card readers and III A programming environment for What is needed to acheive it? How can the attack be conducted? microcontrollers -> Understand the attack -> Oscilloscope and MatLab -> Perform the attack Optional: Presentation of an attack -> Implement a SmartCard on a in the lab on the reference interface -> Streaming server for PayTV microcontroller implementation -> Streaming software as -> Implement countermeasures Python script Practical tasks - Team B -> Relevant standards and brief Final hand-in criterion: description of the lab with Tradeoff evaluation between -> Implement card on Create project plan number of traces needed to Pre-Lab Assignment: microcontroller references to further literature Present project goals Python and AVR tutorials -> GitLab project for version control successfully + Documentation attack the card and the cost of -> Build test environment III B II -> Implement T=0 protocol 16.10.2022 10:00 - 11:30 03.11.2022 13:00 - 14:30



14.12.2022 08:30 - 10:00

26.01.2022 12:00 - 14:00 Oral exam at the beginning of February