國立成功大學
National Cheng Kung University

數論 補充7

計網中心 網路與資訊安全組

李南逸

作業7

- **第一題**

  1. 假設RSA公鑰為(17, 3599)，私鑰為何？若機密訊息為1121，數位簽章為何？
  2. 假設ElGamal的primitive root為10，模數為19，Bob的公鑰為3，私鑰為何？若Bob所選亂數為5，訊息為11，則數位簽章為何？

- **繳交**

  1. Pdf檔案 (可用手算方式完成題目，包含過程，再拍照或掃描成pdf檔案)

  2. 二週內繳交

  3. 一人一組