

---

(注)

- 自分で解くこと．解答用紙を提出．
- 解答が時間内に終了しなかった場合は，解答できなかった問題を宿題とします．
  - 次回の演習終了時まで．
  - 配布した宿題用紙を用いて提出．
- 解答用紙の余白に，質問，感想 (分かりにくかった箇所，良く分かった箇所) などを書いてください．

- 
1. 離散対数問題の困難さに基づく鍵共有方式に Diffie–Hellman 鍵共有がある．手順を説明しなさい．
  2. RSA 暗号によるデジタル署名の手順を説明しなさい．
  3. 公開鍵暗号方式と秘密鍵暗号方式に関する以下の問いに答えなさい．
    - (a) 暗号理論的な観点から，両者の長所・短所について述べなさい．
    - (b) 公開鍵暗号方式と秘密鍵暗号方式のハイブリッド方式とはどのような方式か．
    - (c) ハイブリッド方式が用いられている実際のアプリケーションの例をあげなさい．
-