

---

(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. 擬素数とは何か．カーマイケル数とは何か．簡単に説明せよ．
  2. 91 が擬素数であることを示しなさい．
  3. 離散対数問題とは何か．その困難さとは何か．簡単に説明しなさい．
  4. 離散対数問題の困難さに基づく公開鍵暗号方式に ElGamal 暗号がある．
    - (a) ElGamal 暗号の手順を説明しなさい．
    - (b) ElGamal 暗号が機能することを示しなさい．
-