

---

(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. 以下について説明しなさい．
    - (a) 暗号系のモデル
    - (b) 平文
    - (c) 暗号文
    - (d) 暗号化
    - (e) 復号化
    - (f) 解読
  2. シーザ暗号で暗号化した次の暗号文を復号しなさい．  
QHWHUAVRFVVZHRHUHNVFH
  3. 上杉暗号を用いて，以下の平文を暗号化しなさい．  
「情報理論の単位を落とすべからず」
  4. バーナム暗号で乱数列  
22, 13, 5, 18, 11, 25, 19, 18, 1, 9  
を使った通信により，暗号文  
PUNKTRTHFW  
を受信したとする．これを復号しなさい．
  5. 以下の数を素因数分解しなさい (電卓を用いて良い)．
    - (a) 85
    - (b) 247
    - (c) 154729
    - (d) 337913
    - (e) 1176299
    - (f) 2462561
  6. 次の計算を行いなさい．
    - (a)  $76 \pmod{15}$
    - (b)  $82 \pmod{43}$
    - (c)  $123 \pmod{87}$
    - (d)  $326 \pmod{437}$
-