

---

(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. [再掲] 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．
  2. 鍵配送問題とは何か．説明しなさい．
  3. 公開鍵暗号方式と秘密鍵暗号方式の違いについて述べなさい．
  4. 文字コードを， $_ = 10, A = 11, B = 12, C = 13, \dots, Y = 35, Z = 36$  とする．RSA 暗号における公開鍵を  $e = 61, n = 437$ ，秘密鍵を  $d = 13$  とする．  
このとき，平文 GOOD\_BY を暗号化した結果を求めなさい．
  5. [再掲] 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．[再掲，前回述べた訂正を反映しています]
    - (a)  $76^{15} \pmod{34}$
    - (b)  $82^{43} \pmod{85}$
    - (c)  $123^{45} \pmod{67}$
    - (d)  $326^{61} \pmod{437}$
-