
(注)

- 中間試験を行います。
 - 日時：12 月 06 日 (月) 10:30 ~ 11:30
 - 場所：624 教室 (講義を行っているところ)
 - 範囲：9 月 27 日 (後期第 1 週) ~ 10 月 25 日分
- 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]

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。

2. RSA 暗号法で $p = 19, q = 23$ とする。

- (a) $n = pq$ を求めなさい。
- (b) $p - 1, q - 1$ の最小公倍数 k を求めなさい。
- (c) k と互いに素となる整数 d を選びなさい。
- (d) $ed \equiv 1 \pmod{k}$ を満たす整数 e を求めなさい。
- (e) 上で求めた e, d を用いて、あなたの学籍番号を RSA 暗号化しなさい。

[注] 適宜、ブロックに分割するなどして良い。

3. RSA 暗号が解読されるのはどのような場合か。また、解読されないようにするには、どのようにすれば良いか。
