
(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. RSA 暗号の暗号化・復号化のアルゴリズムを説明し、それがなぜ機能するのかを示しなさい。必要な補題は証明なしに適宜導入してよい。
[ヒント] フェルマーの小定理など。
 2. [再掲] 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。
-