電気通信大学 電気通信学部 情報通信工学科
情報通信工学実験 A・B
実験項目 1. 情報通信「情報・セキュリティ」

本資料は、課題「RSA 暗号の理解と実装 (プログラミング)」[1] を履修するためのポイントをまとめた資料です。

理論面についてポイント

1. 「秘密鍵暗号」と「公開鍵暗号」の主な違いを説明できますか?
   (ヒント: テキストの 2.3 節を参照.)
2. 公開鍵暗号において、「公開鍵」と「秘密鍵」をそれぞれ誰が作成しますか?
   (ヒント: テキストの 2.3 節を参照.)
3. 公開鍵暗号において、「公開する情報」と「秘密にする情報」のそれぞれを説明できますか?
   (ヒント: テキストの 2.3 節を参照.)
4. RSA 暗号において、「公開鍵」と「秘密鍵」を具体的に作成できますか?
   (ヒント: テキストの 4 節を参照.)
5. RSA 暗号において、「公開する情報」と「秘密にする情報」のそれぞれを説明できますか?
   (ヒント: テキストの 4 節を参照.)

実装面についてのポイント (プログラミング言語は C 言語)

1. ファイルを読み書きするプログラムを作成できますか?
   具体的には、1 文字 (1 バイト単位) ずつファイルと入出力する関数「fgetc」と「fputc」を用いて、ファイルを複写 (コピー) するプログラムを作成できますか?
   (ヒント: テキストの 6.2 節の 「2. ファイルをコピーするプログラム」および WEB 資料[2] を参照.)
2. RSA 暗号の暗号化および復号化で行なうベキ乗計算「 $C \equiv M^e \pmod{n}$ 」を実行するプログラムを作成できますか?
   有限桁しか扱えない計算機および C 言語を用いて、大きな整数となってしまうベキ乗計算 M^e をどのように実現するかが問題となる.
   (ヒント: テキストの 4 節の例 4.1 を参照.)
3. 「暗号化における暗号文のファイルへの書き込み」と「復号化における暗号文のファイルからの読み出し」について.

   RSA 暗号の暗号化において、メッセージを 1 バイト単位で暗号化しても、暗号文は 2 バイトになる可能性がある。暗号文が最大で何バイトになるかは、設定した n の値に依存する。たとえば、$(e, n) = (5, 323)$ の場合、 メッセージ $M = 67$ に対し、暗号文は $C = 288$ となる.

   一方、fgetc 関数は、1 バイト単位でしかファイルに書き出すことができない。それでは、fgetc 関数を用いて、暗号文 $C = 288$ をファイルに書き出すにはどうすればよいか?

   1 バイト単位でしか操作できないということを、整数で表現すると $0 \sim 255$ までの数しか扱えないということである.
   (ヒント: テキストの 6.1 節 「プログラミングの準備」の 8, 9 を参照.)

---

[1] 電気通信大学 電気通信学部 情報通信工学科, 情報通信工学実験 A・B, 実験項目 1. 情報通信「情報・セキュリティ」
栗原正純 (E-mail: kuri@ice.uec.ac.jp) (2010/9/24/8:49 作成)
http://www.code.ice.uec.ac.jp/kuri/C3/ (11x3: /doc/tex/uec/jikken/2010/point2010.tex)

[2] http://www.code.ice.uec.ac.jp/kuri/C3/ の参考プログラム