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」

計算シート

本資料は、
1. RSA 暗号の鍵 (公開鍵と秘密鍵) の作成と、
2. 暗号化/復号化の手続き

の理解を助けるための資料です。[1]

1. RSA 暗号の公開鍵 (e, n) と秘密鍵 (d, n) をつくる。

   (a) 200 以下の素数:

   2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101 , 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199.

   (b) 異なる 2 個の素数 p, q を選び、$n := pq$ を計算する。ただし、$256 \leq n \leq 32767$ を満たすような p, q を選ぶ。

   $$p := \_\_\_\_\_, \quad (1)$$
   $$q := \_\_\_\_\_, \quad (2)$$
   $$n := p \times q = \_\_\_\_\_. \quad (3)$$

   ここで、記号 := の意味は、$A := B$ と書いたとき、A は B により定義される。または、同じことだが、B により A を定義することを意味する。

   (c) 上記で選んだ素数 p, q に対し、$p-1$ と $q-1$ の最小公倍数 L :=lcm$(p-1, q-1)$ を計算する。

   $$L := \mathrm{lcm}(p-1, q-1) = \_\_\_\_\_. \quad (4)$$

   最小公倍数を求めるには、整数 x と y の最大公約数 $\gcd(x, y)$ と最小公倍数 $\mathrm{lcm}(x, y)$ の間に成り立つ以下の関係を利用すればよい。

   $$\mathrm{lcm}(x, y) = \frac{xy}{\gcd(x, y)}$$

   ここで、効率良く最大公約数を求めるには、ユークリッド法を利用すればよい。

   (d) 以下の 2 条件を満たす暗号化鍵 (公開鍵) e を求める。

   i. $\gcd(e, L) = 1$,

   ii. $1 < e < L$.

   $$e := \_\_\_\_\_. \quad (5)$$

   (e) 上記で求めた暗号化鍵 e に対し、以下の 2 条件を満たす復号化鍵 (秘密鍵) d を求める。

   i. $e \times d \equiv 1 \pmod{L}$,

   ii. $1 < d < L$.

   $$d := \_\_\_\_\_. \quad (6)$$

   ここで、効率良く秘密鍵 d を求めるには、e と L に対し、拡張型ユークリッド法を利用すればよい。

   (f) 以上の計算により、公開鍵 (暗号化鍵) (e, d) と秘密鍵 (復号化鍵) (d, n) は以下のようになる。

   $$(e, n) := (\_\_\_\_\_, \_\_\_\_\_), \quad (7)$$
   $$(d, n) := (\_\_\_\_\_, \_\_\_\_\_). \quad (8)$$

2. 暗号化と復号化の計算をする。

   (a) アルファベットの平文：

   $M_{\text{平文}} := \_\_\_\_\_$.

   (b) 上記の $M_{\text{平文}}$ を ASCHII コードで 10 進数に変換する：

   $M := \_\_\_\_\_$.

   (c) (暗号化) 公開鍵 (e, n) を用いて、M に対する暗号文 C を計算する。

   $$C \equiv M^e \equiv \_\_\_\_\_ \pmod{n} \quad (9)$$

   (d) (復号化) 秘密鍵 (d, n) を用いて、暗号文 C に対する推定平文 $\widehat{M}$ を計算する。

   $$\widehat{M} \equiv C^d \equiv \_\_\_\_\_ \pmod{n} \quad (10)$$

   (e) (確認) 平文 M と推定平文 $\widehat{M}$ が一致するか確認する。

[1] ©電気通信大学 情報通信工学専攻 栗原正純 (E-mail: kuri@ice.uec.ac.jp) 2011. (2011/10/31/12:29 作成)

ポイント

本資料は、課題「RSA 暗号の理解と実装 (プログラミング)」を履修するためのポイントをまとめた資料です。[2]

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[3] 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.)

[2] ©電気通信大学　情報通信工学科栗原正純　(E-mail: kuri@ice.uec.ac.jp) 2010-2011. (2011/10/31/12:29 修正)

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