10 進数を基とした任意桁整数演算ライブラリの構築及び，

それを用いたRSA システムの実装

975121　鈴木 智裕

（指導教員　速水 治夫 教授）

1．まえがき

プログラミング言語であるC 言語では，整数を扱う際に標準の整数型では表現の限界がある．それ以上の大きさの整数を扱うためには，多倍長整数演算ライブラリ等を使用するすることになるが，プログラミング初学者には敷居が高い．そこで本研究では，100 桁を超える整数の演算を行えるライブラリを構築する．そして，その構造を，プログラミング初学者にも理解と応用を行うことが容易なものとする．また，本ライブラリを使用して RSA 暗号システムを実装し，その有用性を確認する．

2 C 言語における整数

標準的な C 言語における整数型には，char 型・short int 型・long int 型が存在し，その表現できる数値の限界は 32 ビットであり，10 進数において10 桁程度である．処理系により，その倍の64 ビットの大きさを持つ long long 型を使用したとしても，その表現できる最大の整数は，10 進数においてたかだか 20 桁程度しか表現できない．また，実数型での代用を考えれば，たしかに 30 桁を超える巨大な数値を扱うことができるが，整数演算に使用するには常に誤差に気を配らねばならず，さらに有効桁に至っては 15 桁程度にまで低くなる．

3 RSA 暗号システム

暗号方式の一種であり，公開鍵暗号方式の先駆けとして広く知られている．巨大な素数を扱うことにより強度が増す形態をとっており，整数演算が要となるため，本研究の実用評価用として採用した．

4 システムの概要

数値の表現には signed char 型の配列を用いる．数値の10 進数における各 1 桁の値を，その桁数と一致する要素番号を持つ要素へ格納するという形式をとることにより，変数の内部構造が理解しやすく，応用しやすい．また，整数演算を行うことを前提とするため，比較演算や四則演算・剰余などの基本的な整数演算を行う関数群を用意するほか，累乗，倍数・約数，素数などに関連する関数群も用意した．各関数群の引数は，C 言語における一般的な数式の並びを模倣しており，直感的に判り易い．

5 システムの特徴

- 全ての関数は“gi_”で始まるため，他のライブラリ関数との見分けが容易である．
- 機種依存するような関数は使用しないため環境を選ばず，DOS，Windous，UNIX のどの環境でも使用が可能である．
- メモリの管理はシステム側で行うため，使用者の労力を軽減し，エラーの発生を抑える．

6．まとめ

本研究により 1 万桁を超える数値の整数演算を行うことができ，その有用性を確認できた．しかし，MS-DOS ではメモリの仕様上 5 千桁が限界であった．

RSA 暗号システムによる評価では，実時間で実行するために利用桁数を抑えて稼動させるため，使用可能桁数を十分に活用できない．速度面での課題が残る．