# 暗号理論を題材とした情報処理教育の一考察[1]

2X－4

柴木 恒一　芳賀 久人　大須賀 錬太郎　菅原 光政
岩手県立大学宮古短期大学部　(株)ネクスト・システム開発部　岩手県立大学ソフトウェア情報学部

## 1.はじめに

短期大学における情報処理教育の一環として，学生に暗号理論の入門的内容を理解し興味をもたせることを目標としている．そのために，RSA 暗号の実装と評価を題材とする教育を行った．これにより，暗号理論に必要な数学的手法，プログラミングとアルゴリズムの習熟，暗号理論に対する興味等の促進効果が得られた．本稿では，教材の選定から教育プロセスを概観し，実装されたプログラムの学生自身の評価に基づく教育的考察を行う．

## 2.教材について

### 2.1 題材の選定

身近に暗号を体験させ一層の理解を深めることが，暗号の実装と評価を題材とした理由である．そのため，学生の興味の引き易さという点から，公開鍵暗号を設定し，比較的実装が容易で，ユークリッドの互除法，合同式，フェルマーの小定理，素数判定等の暗号理論に必要な数学的手法を学べることから，RSA 暗号を選択した．これは，オイラーの定理，中国剰余定理，さらには群，環，有限体論等の一般論を学ぶ足掛りとなる．

### 2.2 プログラミング言語の選定

プログラミングの入門レベルの学生が，前期2単位，後期4単位の授業という限られた期間で学習することを想定しているため，第一にプログラミング言語の修得に時間を取られないことが要件となる．またできるだけ現実味のある暗号変換を体験させるために，使用可能な文字種類と暗号化する文字ブロックを可能な限り大きくとりたい．そのためには，変数の扱える整数値の範囲ができるだけ大きいプログラミング言語を選ぶ必要がある．これが第二の要件である．

これらの要件を十分充たすものとして，UBASIC を選んだ．UBASIC は，形式は BASIC 言語に準じているので第一の要件を充たす．また整数値の変数は，-65536^542～65536^542(10 進で 2600 桁強)の数値を扱えるため第二の要件も充たすと考えられる．

## 3.教育プロセス

暗号理論の理解と興味付けを目的として前述の題材による講義の教育プロセスを示す．

**実施期間**：平成9年4月～平成10年3月

**講義名**：基礎研究，特別研究Ⅰ，特別研究Ⅱ

**講義形態**：基礎研究，特別研究Ⅰはゼミ形式．
特別研究Ⅱは演習及び課題リポート作成．

**提出課題**：「RSA 暗号の実装と評価」
(特別研究Ⅱでの課題リポート)

今回実施した教育では，基礎研究及び特別研究Ⅰを 5 名の学生が受講し，そのうち特別研究Ⅱを受講した 2 名の学生が課題を提出した．

**教育内容**：

| 科目・方針・使用ﾃｷｽﾄ | 教育内容 |
|---|---|
| **科目**：基礎研究<br>(前期2単位 選択科目)<br>**方針**：RSA 暗号の仕組みの理解に必要な情報数学を学ばせ，理論を裏付ける実例をｺﾝﾋﾟｭｰﾀで計算させる．<br>**使用ﾃｷｽﾄ**：文献[1]，[2] | 第1週～第4週：ﾕｰｸﾘｯﾄﾞの定理とその適用例<br>第5週～第6週：算術の基本定理(素因数分解の一意性)<br>第7週～第8週：ﾕｰｸﾘｯﾄﾞ・ｱﾙｺﾞﾘｽﾞﾑ<br>第9週～第10週：ﾕｰｸﾘｯﾄﾞ・ｱﾙｺﾞﾘｽﾞﾑの応用(拡張されたﾕｰｸﾘｯﾄﾞ・ｱﾙｺﾞﾘｽﾞﾑ)<br>第11週：UBASIC の使用説明<br>第12週～第13週：ﾕｰｸﾘｯﾄﾞ・ｱﾙｺﾞﾘｽﾞﾑ，拡張されたﾕｰｸﾘｯﾄﾞ・ｱﾙｺﾞﾘｽﾞﾑのﾌﾟﾛｸﾞﾗﾐﾝｸﾞ<br>(第1週～第10週まで文献[1]を輪読．第11週は文献[2]に基づいた講義．第12週～第13週では，UBASIC によるﾌﾟﾛｸﾞﾗﾐﾝｸﾞ実習．) |
| **科目**：特別研究Ⅰ<br>(後期2単位 必修科目)<br>**方針**：基礎研究に引き | 第1週：n 以下の自然数の中に含まれる素数の個数<br>第2週：素数表の作り方(ｴﾗﾄｽﾃﾈｽの篩 |

[1] Consideration to Information Processing Education Using Cryptography
Koichi Shibaki
Miyako Collage, Iwate Prefectural University

| | |
|---|---|
| 続き RSA 暗号の仕組みの理解に必要な情報数学を学ばせ，最後に RSA 暗号の仕組みを学習させる.<br>**使用ﾃｷｽﾄ**：文献[1] | による)<br>第 3 週～第 4 週：素因数分解の初歩的な方法<br>第 5 週～第 6 週：完全数<br>第 7 週：ﾒﾙｾﾝﾇ素数<br>第 8 週：ﾌｪﾙﾏｰの小定理<br>第 9 週：擬素数<br>第 10 週：高速冪乗計算法<br>第 11 週～第 12 週：ｵｲﾗｰの定理<br>第 13 週～第 14 週：ﾒﾙｾﾝﾇ素数のｵｲﾗｰの定理から導かれる性質<br>(第 1 週～第 13 週まで文献[1]を輪読. ) |
| **科目**：特別研究Ⅱ<br>(後期 2 単位 選択科目)<br>**方針**：前半は特別研究Ⅰの補充として，RSA 暗号の仕組に関連した資料を読ませ，後半は課題「RSA 暗号の実装と評価」をさせる.<br>**使用ﾃｷｽﾄ**：文献[3], [4], [5], [6], [7] | 第 1 週～第 9 週：文献[3], [4], [5], [6], [7]で RSA 暗号の仕組みに必要な箇所の輪読<br>第 10 週～第 11 週：RSA 暗号のﾌﾟﾛｸﾞﾗﾐﾝｸﾞ実習<br>第 12 週～第 14 週：課題ﾘﾎﾟｰﾄの作成<br>以降，実装への自主的な取り組みとその評価 |

## 4. 実装内容と評価

学生による RSA 暗号の実装では，2 つの大きなメルセンヌ素数 2^107－1 (33 桁)，2^127－1 (39 桁)の積に基づいて RSA 暗号を構成し，暗号化できる文字ブロックは，半角 30 文字，使用できる文字種類は，カタカナ，大文字アルファベット，句読点を含む 100 文字という仕様になった. また通常の RSA の暗号化・復号化は，

**暗号化**:平文 → 非負整数 → 暗号化非負整数 → 暗号文
ラベリング　暗号化変換　ラベリング逆対応

**復号化**:暗号文 → 暗号化非負整数 → 非負整数 → 平文
ラベリング　復号化変換　ラベリング逆対応

といった手順で変換が行われるのに対し，学生の行ったものは，

**暗号化**:平文 → 非負整数 → 暗号化非負整数
ラベリング　暗号化変換

**復号化**:暗号化非負整数 → 非負整数 → 元の平文
復号化変換　ラベリング逆対応

と簡略化されたものとなった. 但し，RSA 暗号の本質的な部分の実装化には成功している.

さらに，学生自身のプログラムに対する評価・問題点は主に，

①メルセンヌ素数を用いる RSA 方式では，暗号が破られ易いので，それらを除く大きな素数たちを採用すべきでなかったか.

②このプログラムでは，二つペアの公開鍵のうち一つをあらかじめプログラムに組込み，残る一つをキーボード入力するという方法を採っている. 入力ミスや手間を考えると二つの鍵をファイルから直接読み込む方法にすべきでなかったか.

というものであった.

以上のような学生の報告から，「RSA 暗号の実装と評価」といった課題の試みは，暗号化技術を学うえで必要な様々な数学的手法を修得でき，プログラミングやアルゴリズムに対する良い練習問題となりえた. さらに文字単位が 30 文字という比較的長い仕様の RSA 暗号を，学生たちが短期間にプログラム化したことは，使用言語の特性に支えられるところが大きいと考えられる. そして，学生による実装後の評価によって，自らのプログラムの問題点や改善点を示唆し得ることは，この試みが暗号理論の興味と理解を深めるための恰好の教材であると考えられる.

## 5. おわりに

本稿では，「RSA 暗号の実装と評価」を題材に使った教育の実例とその効果を考察してきた. この試みから派生する暗号理論上の教育課題は広範囲に広がっていくと考えられる. その一つ一つを今後の暗号理論に関する情報処理教育で取り上げ改善工夫することで，学生の暗号理論への理解と興味を深める手段としていきたい.

## 参考文献

[1] David.M.Bressond, Factorization and Primality Testing, Springer-Verlag, 1981, 1-57.

[2] 木田 祐司, UBASIC86/多倍長計算用 BASIC 題 8.3 版 ユーザーズマニュアル, 日本評論社, 1992.

[3] Neal Koblitz, 桜井 幸一訳, 数論アルゴリズムと楕円暗号理論入門, シュプリンガー・フェアラーク東京, 1997, 115-113.

[4] 一松 信, 暗号の数理 - 作り方と暗号の原理 -, 講談社, 1997, 125－215.

[5] 今井 秀樹, 暗号のおはなし - 情報セキュリティーの新しい鍵 -, 日本規格協会, 1996, 84-95.

[6] 松坂 和夫, 代数系入門, 岩波書店, 1995, 9-38.

[7] 戸川 隼人他編, bit 別冊インターネット時代の数学, 共立出版, 1997, 196-201.