研究テーマ：RSA 暗号～素数の判定～

名列番号　０５６　　**氏　　名**　　藤岡　久範

1. まえがき

RSA は現在主流の暗号方式である。

2. 研究課題

RSA 暗号の解読の困難性は大きな数字の素因数分解の困難性に起因する。そこで、暗号の要となる素数を得る手法や効率を調査、解析する。

3. 研究方法

素数を得る手法として以下の３つを採用する。

- 素数の定義から求める方法（素数判定法（方法１））判定回数が多くなるので、素数の１の位の数字がある程度固定されることを利用した方法２も実行する。
- Miller-Rabin 法（素数判定法）
- エラトステネスのふるい（素数獲得法）

4. 実験と考察

方法１，２による判定回数の変化を表１に、「ふるい」によって得られた素数でさらに Miller-Rabin 法にかけて素数と判定された数の個数を表２に示す。方法２では、反復領域を大きく取りすぎると、かえって効率が悪くなることもあった。Miller-Rabin 法では、扱う数字が大きいとうまく判定されなかった。

奇数 n の桁数	方法１[回]	方法２[回]
4	10^3	10^2
5	10^4	10^3
6	10^5	10^4
7	10^6	10^4
8	10^7	10^5

表１　判定回数の変化

素数の大きさ（桁）	素数の数（ふるい）	素数の数（M-R 法）
1	4	4
2	21	21
3	143	18
4	1061	判定不可
5	8363	判定不可
6	68906	判定不可
7	586081	判定不可

表２　素数の分布

5. まとめと感想

素数の定義から求める方法
→確定的に求まるが判定に時間がかかる
Miller-Rabin 法
→確率的にしか求まらない
エラトステネスのふるい
→領域内の全素数を求められるが、時間、メモリ的に無駄がある
期待する結果が得られないことがあったが、そこからの究明の大切さを知った。素数は奥深い。

6. 参考文献

[1]情報処理学会監修「暗号・ゼロ知識証明・数論」共立出版
[2]http://www.nara-edu.ac.jp/
(Miller-Rabin 法のアルゴリズムについて)
[3]http://www.fukagawa.com/
(Miller-Rabin 法判定の証明について)