コンピュータとインターネット時代の

数値シュミレーションと暗号技術で
未来を拓く

コンピュータ応用学科

オープンキャンパス:暗号解読に挑戦

体験イベント(2/5)

因数分解に挑戦

1. 素数の判定と因数分解

(1) 素数の判定

素数の判定法は 2002 年に決定的方法が考案されました。ただ、高速に判定するには確率的な方法が使用されます。確率的方法では、1 回の評価で 1/2 の比率で素数らしさが増していきます。ここでは 10 回評価して素数と判定していますので、99.9%の確率で素数となっています。

(2) 因数分解

因数分解の方法は多数考案されています。因数分解する値の平方根の値までの素数で、因数分解する方法は単純ですが、10 進 60 桁の分解に 10^{30} の計算量が必要で、これは最先端のスーパーコンでも数億年かかります。ここでは、10 進 100 桁位まで高速な解法である MPQS(複数多項式 2 次ふるい法)で因数分解に挑戦します。この方法なら、10 進 60 桁の合成数の分解はパソコンで数秒から数十秒で分解できます。この方法でも分解する数が 10 桁長くなると、計算時間は 10 数倍多くかかります。そのため、RSA 暗号に使用されている 1024 ビット(10 進 309 桁)の合成数の分解には、最先端のスーパーコンでも数千年かかります。それで、RSA 暗号は安心して使用できます。

2. 因数分解に挑戦

(1) 2 個の素数で合成数を作成

Java で作成 prime2 を使用して、n ビットの 2 個の素数を作成し、それを乗算して 2n ビット(10 進 0.6n 桁)の合成数を作成します。ファイル：Open7-20/RSA

(a) コマンドプロンプトを立ち上げる

(b) cd Open7-20/RSA

(c) java Prime2

(d) 2 個の素数の長さ(ビット数)を画面から与える → 合成数(乗算結果)が画面上に表示される

(2) 合成数の因数分解

C 言語で作成した factor.exe を使用して因数分解。

(a) input.txt に Prime2 で得られた合成数を与える

(b) factor.exe をダブルクリック

(c) factor.txt に素因数分解結果が得られる

(注) 画面上に表示された文字を input.txt にコピーする方法

(a) 画面上の任意の位置 → 右クリック → 範囲指定
→ 左クリックし、コピーする文字を左から右に移動 → Enter

(b) input.txt を開く → コピーする位置 → 編集 → 貼り付け

3. 実施例

(1) 2 個の素数で合成数を作成

(a) Input bitsize = 80

110091612231284356286960 3 * 961959224128264992744643

= 105903641885036107741235590022419589502408578672 9

(b) Input bitsize = 100

113089676038610519684979704740 3 * 839155113871121473638332403799

= 948997799738284482532738740659045234888169216233049740283997

(c) Input bitsize = 120

112098814022528776318119710482767885 7 * 678712075407339723831584043434257127

= 760828187159319024678668613341497680076959970143155648372864501519463839

(2) 合成数の因数分解

計算時間はインテル® Core™2 Duo (1.87Gh)を使用して測定。

(a) 10 進 49 桁(160 ビット)の分解

factoring 105903641885036107741235590022419589502408578672 9

prp24 factor: 961959224128264992744643

prp25 factor: 110091612231284356286960 3

elapsed time 00:00:01

(b) 10 進 60 桁(200 ビット)の分解

factoring 948997799738284482532738740659045234888169216233049740283997

prp30 factor: 839155113871121473638332403799

prp31 factor: 113089676038610519684979704740 3

elapsed time 00:00:10

(c) 10 進 72 桁(240 ビット)の分解

factoring 760828187159319024678668613341497680076959970143155648372864501519463839

prp36 factor: 678712075407339723831584043434257127

prp37 factor: 112098814022528776318119710482767885 7

elapsed time 00:02:19