コンピュータとインターネット時代に
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 **数値シミュレーション研究室**

研究内容 RSA暗号解読の高速計算方式の研究

1. 多数桁の因数分解（世界記録の因数分解、10 進 200 桁、2005 年）

279978339112213278708294676387226016210704467869554285375600099293261284001076093456710529553608560618223519109513657886371059544820065767750985805576135790987349501441788631789462951872378692218239832 = 353246193440277012127260497819846436867119740019762502364930346877612125367942320005854795652808834 9 × 792586995447833033347085841480059687737975857364219960734330341455767872818152135381409304740185467

2. RSA 暗号化と復号

準備　：素数 P,Q,e を選ぶ。n=P×Q, d=1/e (mod (P-1)×(Q-1))を計算。e,n は公開鍵、d は秘密鍵とする。
　　現在 P,Q は 10 進 154 桁と 155 桁で n は 309 桁(1024 ビット)のものが使用されている。
暗号化：$C=M^e \pmod n$で整数 M を整数 C に変換する。(mod n)は n で割った余りを示す。
復号　：$M=C^d \pmod n$で整数 C を元の整数 M に変換する。オイラーの定理によりこの計算で元の数に戻る。

3. 復号と解読

復号：　秘密鍵 d を使用して暗号を元の数に変換する。高速な方が良い。
解読：　秘密鍵 d を知らないで暗号から元の数に変換する。

4. 解読(多数桁の因数分解)

RSA 暗号が安全に使用できるためには、暗号強度(暗号の解読に要する時間)を常に確認し、暗号設計に反映させることが重要である。

(1)　総当り因数分解（平方根以下の全ての素数で割り算）
　309 桁の因数分解にスーパーコンで 10^{132} (1 兆×1 兆×…×1 兆と 11 回兆を掛ける)年かかる。

(2)　現在の因数分解の計算方法
　複数多項式 2 次ふるい法(MPQS)：　309 桁の因数分解にスーパーコンで 10 万年かかる。100 桁までは GNFS より高速。
　一般数体ふるい法(GNFS)　　：　309 桁の因数分解にスーパーコンで 1000 年かかる。

(3)　RSA 暗号の因数分解の世界記録
　RSA-100(10 進 100 桁の因数分解)：　1991 年 4 月
　RSA-120(10 進 120 桁の因数分解)：　1993 年 1 月
　RSA-140(10 進 140 桁の因数分解)：　1999 年 2 月
　RSA-160(10 進 160 桁の因数分解)：　2003 年 4 月
　RSA-200(10 進 200 桁の因数分解)：　2005 年 5 月

(4)　研究室での取り組み

(a)　新解法の考案と評価
　MBPS(多重基底多項式ふるい法)を考案し、プログラム作成中
　N: 分解対象数 → $f(x)=Ax^2+Bx+C$, $f(M)=N$ となる整数 A,B,C 及び M を求める。
　　$g(x)=(A_1x+a)(A_2x+b)-f(x)=Sx+T=G(sx+t)$
　　$A_1A_2=A$,　$S=A_1b+A_2a-B$,　$T=ab-C$,　$G=GCD(|S|,|T|)$
　　a,b の値は GNFS(一般数体ふるい法)を使用して選定する。
　目標: RSA-768 の因数分解で GNFS の 100 倍の高速化

(b)　RSA-768(10 進 232 桁の因数分解)への挑戦
　2 年後に MBPS で RSA-768 を因数分解することを目標にしている。
　そのときの、行列サイズは 2 億次元になると予測される。
　2 億次元の 0-1 行列から従属行の計算には疎行列直接解放（ダイレクトソルバー）を使用する。

RSA-768=123018668453011775513049495838496272077285356959533479219732245215172640050726365751874520219978646938995647494277406384592519255732630345373154826850791702612214291346167042921431160222124047927473779408066535141959745985690214341 3