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

暗号解読に挑戦

体験イベント(4/5)

1. RSA 暗号の強度

RSA 暗号の強度は合成数 N の長さに依存します。現在使用されている RSA 暗号では N は 1024 ビット(10 進 309 桁)です。この長さの N(鍵)ですと最先端のスーパーコンでも解読に数千年かかります。しかし、N を短く し、10 進 60 桁程度にすると、パソコンでも簡単に解読可能になります。RSA 暗号の解読のためには、N を素数の積に因数分解する必要があります。ここで使用する因数分解の方法は MBPS(複数多項式 2 次ふるい法)です。暗号解読とは、復号鍵(e)を使用しないで元のメッセージに戻すことです。

2. 暗号解読の方法

(1) 暗号化

体験イベント(3/5)で使用した java RSA でメッセージを暗号化します。

(2) N の因数分解

上記暗号化で使用した N を体験イベント(2/5)で使用した factor.exe で因数分解します。

通常はこれが不可能なために、暗号解読ができません。

(3) 暗号解読

Java で作成した Decode を使用して暗号解読をします。ファイル：Open7-20/RSA

(a) コマンドプロンプト→ cd Open7-20/RSA → java Decode

(b) 画面から解読する暗号を入力

(c) 画面から暗号化に使用した e を入力

(d) 画面から N を分解する 2 つの数を入れる

(e) 画面に解読されたメッセージが表示される

3. 実施例

解読する暗号を入れてください

476502091529051533723661311595619651363439192740 9

e を入れてください

154438565299687982782710182298080715308846408557 1

N を分解する 2 つの数を入れてください

297799007338735668947754 7 ： factor.exe で N を分解した最初の値

439785015313266142040006 3 ： factor.exe で N を分解した 2 番目の値

N: 13096754100274132238157258155216847522399195885461

e: 154438565299687982782710182298080715308846408557 1

d: 10184671353331750480410440139502476591580044322319

解読数: 70243974392724742420373927742334243874323441247 2

解読メッセージ: Yet the earth does move.