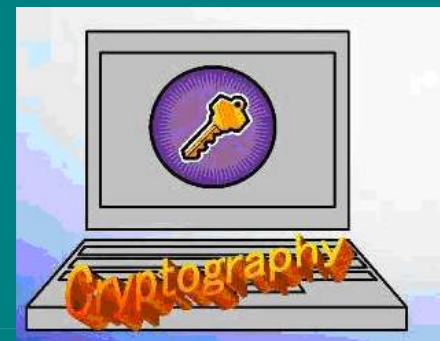


# コンピュータとインターネット時代の 数値シミュレーションと暗号技術で 未来を拓く



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 暗号化と復号化

体験イベント(3/5)

### 1. RSA 暗号の仕組み

準備 : 素数  $P, Q, e$  を選ぶ。  $N = P \times Q$ ,  $d = 1/e \pmod{(P-1) \times (Q-1)}$  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。 $\pmod{N}$  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。

文字変換 : RSA 暗号は整数  $M$  を対象にします。そのため、文章を整数  $M$  に変換及び整数  $M$  を文章に逆変換する処理も必要になります。

### 2. 暗号化と復号化

Java で作成した RSA を使用して、英数字の文章を暗号化し、またそれを復号化して元の文章に戻します。

ファイル : Open7-20/RSA

- (1) コマンドプロンプトを立ち上げる
- (2) `cd Open7-20/RSA`
- (3) `java RSA`
- (4) 画面から暗号化する文章の最大文字数を入れる
- (5) 画面から暗号文 (英字、数字、スペース及び. , で作成)を入れる
- (6) 暗号化し、またそれを復号化したものが画面に表示される

### 3. 実施例

最大文字数を入れてください

25

$N$ : 13096754100274132238157258155216847522399195885461 : 毎回異なる

$e$ : 1544385652996879827827101822980807153088464085571 : 毎回異なる

最大文字数以内の英数字を入れてください

Yet the earth does move. : 入力メッセージ

変換数: 702439743927247424203739277423342438743234412472 :  $M$

暗号文: 4765020915290515337236613115956196513634391927409 :  $C$

$d$ : 10184671353331750480410440139502476591580044322319

復号数: 702439743927247424203739277423342438743234412472 :  $M$

復号メッセージ: Yet the earth does move.