平成 22 年度　自主課題研究

RSA 暗号の実装およびその応用

電子情報学類　情報システムコース　3 年 219 番　金　裕一郎

238 番　中村　裕樹

## 1.　目的

RSA 暗号は、公開鍵暗号系として世界で初めて公開された暗号化を行うアルゴリズムである。実際に RSA 暗号化、復号化を行うプログラムを作成し、その動作を確認することで RSA 暗号についての知識を深めることを目的とする。

## 2.　開発環境

数式処理ソフト Mathematica を使用した。

## 3.　概要

RSA 暗号を実行するうえで必要な値は

・素数 p、q

・n=p×q

・(p-1)(q-1)と互いに素である数 e

・(p-1)(q-1)を法とする e の逆元 d

である。

また、メッセージを図 1 のようにした。

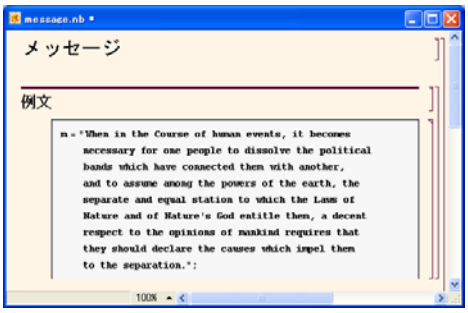


図 1　メッセージ

RSA 暗号化、CBC モードを導入したもの RSA 暗号化の実行結果はそれぞれ図 2、図 3 のようになった。

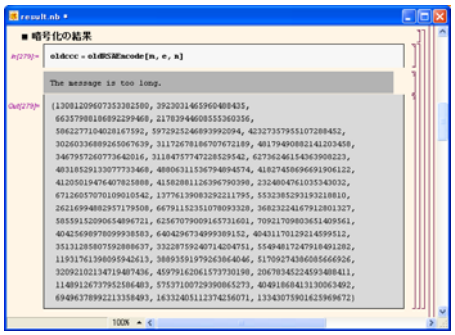


図 2　RSA 暗号化

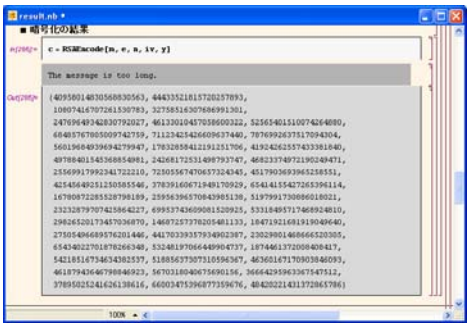


図 3　CBC モードを導入した RSA 暗号化

ガウス整数を用いた RSA 暗号化には条件が存在し、その条件は p≡1(mod 4) かつ q≡1(mod 4) である。また、ガウス整数を用いた RSA 暗号化のメッセージは「GaussianUsed」であり、実行結果は図 4 のようになった。

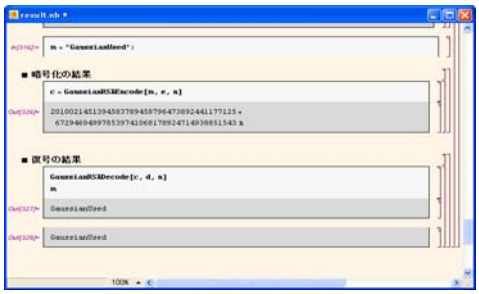


図 4　ガウス整数を用いた RSA 暗号化

どの暗号化においても、復号するとメッセージが復号された。