令和４年度卒業研究概要

RSA 公開鍵暗号とエル・ガマル暗号

中等教育教員養成課程　数学専攻　吉川 颯斗

本論文の目標は, 素因数分解の難しさを利用した RSA 公開鍵暗号と, 離散対数問題の難しさを利用したエル・ガマル暗号という 2 つの公開鍵暗号を解説することである.

RSA 公開鍵暗号とは次のような暗号である. 異なる 2 つの大きな素数 p と q を用意し, $m = pq$ として $\varphi(m)$ と互いに素な数 k を用意する. そしてこの数 k と m を公開し, p と q を秘密鍵とする. 暗号化, 復号化は次の通りである.

暗号化. 以下の 3 ステップで行う.

STEP1 : 送りたいメッセージを数の列に変換する.

STEP2 : 数の列を m 未満になるように区切り, 数のリスト $a_1, \ldots, a_r$ を得る.

STEP3 : $a_1^k (\mathrm{mod}\ m), \ldots, a_r^k (\mathrm{mod}\ m)$ を計算し, 数のリスト $b_1, \ldots, b_r$ を得る.

復号化. 以下の 3 ステップで行う.

STEP1 : $\varphi(m) = (p-1)(q-1)$ を計算する.

STEP2 : $x^k \equiv b_i (\mathrm{mod}\ m)$ を解き, 元の数のリスト $a_1, \ldots, a_r$ を得る.

STEP3 : リストをアルファベットのメッセージに戻す.

また, エル・ガマル暗号とは次のような暗号である. 大きな素数 p と, p を法とした原始根 g, 自然数 k を用意し, $a \equiv g^k (\mathrm{mod}\ p)$ を計算する. そしてこの数 a と g を公開し, k を秘密鍵とする. 暗号化, 復号化は次の通りである.

暗号化. 以下の 4 ステップで行う.

STEP1 : 送りたいメッセージを数の列に変換する.

STEP2 : 数の列を p 未満になるように区切り, 数のリスト $m_1, \ldots, m_t$ を得る.

STEP3 : それぞれに対し, ランダムに $r_1, \ldots, r_t \in \mathbb{Z}$ を決める.

STEP4 : $x_i \equiv g^{r_i} (\mathrm{mod}\ p), y_i \equiv m_i a^{r_i} (\mathrm{mod}\ p)$ を計算し, t 個の数の組 (x_i, y_i) を得る.

復号化. 以下の 4 ステップで行う.

STEP1 : $c_i \equiv x_i^k (\mathrm{mod}\ p)$ を計算する.

STEP2 : $c_i u_i \equiv 1 (\mathrm{mod}\ p)$ を u_i について解く.

STEP3 : $v_i \equiv u_i y_i (\mathrm{mod}\ p)$ を計算し, 数のリスト $v_1, \ldots, v_t$ を得る.

STEP4 : リストをアルファベットのメッセージに戻す.