

アルゴリズム論特論 (塩田)

— RSA 暗号の復習 —

- 鍵 :
- p, q : 大きな素数 (合わせて 1000 ビット程度)
 - $n = pq$
 - $m = (p - 1)(q - 1) = \varphi(n)$
 - e : m と互いに素な正整数
 - $d = e^{-1} \bmod m = \text{modinv}(e, m)$

このうち

- 公開鍵 : e, n
- 秘密鍵 : p, q, m, d

RSA 暗号システム : $P \xrightarrow{E} C \xrightarrow{D} P$

- 平文の集合 P 、暗号文の集合 C はともに

$$P = C = \mathbf{Z}/n\mathbf{Z} = \{x \mid 0 \leq x \leq n - 1\}$$

- 暗号化関数 : $E(x) = (x^e, \bmod n) = \text{modpower}(x, e, n)$
- 復号化関数 : $D(y) = (y^d, \bmod n) = \text{modpower}(y, d, n)$
- 送信者はメッセージ $x \in P$ を $y = E(x)$ に変換して送信する。
- 受信者は暗号文 $y \in C$ を $D(y)$ によって復号する。

-
- $D(E(x)) = x$ となることは前回確かめた。
 - 今日はいは
 - RSA 暗号の安全性の根拠
 - 使ってはいけない危険な鍵