

RSA 暗号 (素数の性質を用いた公開鍵暗号)

鍵の作り方

1. 2つの素数 p, q を選びます。
 2. $n = pq$ を計算します。(公開鍵 n)
 3. $\ell = (p - 1)(q - 1)$ を計算します。
 4. ℓ と互いに素な整数 e を選びます。(公開鍵 e)
 5. d, k についての一次不定方程式 $ed - k\ell = 1$ を解きます。(公開鍵 d)
- e, n を友達に公開し、 d を自分だけの秘密にします。 p, q は破棄してください。

メッセージの暗号化、復号の仕方

(暗号化) 送信者は送る相手の公開鍵 e と n を用いて暗号化します。メッセージ m を e 乗した数を n で割り、その余りを暗号文 c とします。

メッセージ m 相手の公開鍵 e 相手の公開鍵 n m の e 乗を n で割った余り

$$\boxed{}^{} \bmod \boxed{} = \boxed{} \leftarrow \text{暗号文 } C$$

(復号) 受信者は自分の公開鍵 n と秘密鍵 d を用いて復号します。受け取った暗号文 c を d 乗して公開鍵 n で割ります。その余りがもとのメッセージ m となります。

暗号文 c 自分の秘密鍵 d 自分の公開鍵 n c の d 乗を n で割った余り

$$\boxed{}^{} \bmod \boxed{} = \boxed{} \leftarrow \text{もとのメッセージ}$$

----- \dagger ----- \uparrow ----- \downarrow ----- \uparrow ----- \downarrow -----

の公開鍵 $e =$ $n =$.