

「公開鍵暗号システム」としての RSA暗号の説明用資料

2009/06/11作成

RSA暗号

公開

暗号化鍵

$$(e, n) = (5, 323)$$

RSA暗号

公開

暗号化鍵

$$(e, n) = (5, 323)$$

RSA暗号

公開

暗号化鍵

$$(e, n) = (5, 323)$$

RSA暗号

公開

暗号化鍵
 (e, n)

RSA暗号

公開

暗号化鍵
 (e, n)

RSA暗号

公開

暗号化鍵
 (e, n)

RSA暗号

秘密

復号化鍵

$$(d_e, n) = (29, 323)$$

RSA暗号

秘密

復号化鍵

(d_e, n)

RSA暗号

秘密

$$(p, q) = (17, 19)$$

$$d_e = 29$$

RSA暗号

秘密

$$(p, q)$$
$$d_e$$

RSA暗号

メッセージ

WEWILLMEETATCHOFASTATION

RSA暗号

メッセージ

WEWILLMEETATCHOFASTATION

RSA暗号

暗号文

$S_g S_c g g^{2^L} W^{2^L} c_l$

RSA暗号

暗号文

$S_g S_c g g^{2^L} W^{2^L} c_l$

RSA暗号

暗号文

$S_g S_c g g^{2^L} W^{2^L} c_l$

Aさん

Bさん

Cさん

公開通信路