「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

WEWILLMEETATCHOFUSTATION

RSA暗号

メッセージ

WEWILLMEETATCHOFUSTATION

RSA暗号

暗号文

SgScgg2^L2 W2^L2cl

RSA暗号

暗号文

SgScgg2^L2 W2^L2cl

RSA暗号

暗号文

SgScgg2^L2 W2^L2cl

Aさん

Bさん

Cさん

公開通信路