

# 「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

2009/6/11

栗原正純 電気通信大学

1

## RSA暗号

## 公開

## 暗号化鍵

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

2009/6/11

栗原正純 電気通信大学

2

# RSA暗号

## 公開

### 暗号化鍵

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

2009/6/11

栗原正純 電気通信大学

3

# RSA暗号

## 公開

### 暗号化鍵

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

2009/6/11

栗原正純 電気通信大学

4

# RSA暗号

## 公開

# 暗号化鍵 $(e, n)$

2009/6/11

栗原正純 電気通信大学

5

# RSA暗号

## 公開

# 暗号化鍵 $(e, n)$

2009/6/11

栗原正純 電気通信大学

6

# RSA暗号

## 公開

# 暗号化鍵 $(e, n)$

2009/6/11

栗原正純 電気通信大学

7

# RSA暗号

## 秘密

# 復号化鍵

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

2009/6/11

栗原正純 電気通信大学

8

# RSA暗号

秘密

復号化鍵  
 $(d_e, n)$

2009/6/11

栗原正純 電気通信大学

9

# RSA暗号

秘密

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

$d_e = 29$

2009/6/11

栗原正純 電気通信大学

10

# RSA暗号

秘密

$(p, q)$

$d_e$

2009/6/11

栗原正純 電気通信大学

11

# RSA暗号

メッセージ

WE WILL MEET AT THE FUSTATION

2009/6/11

栗原正純 電気通信大学

12

# RSA暗号

## メッセージ

WE WILL MEET AT THE STATION

2009/6/11

栗原正純 電気通信大学

13

# RSA暗号

## 暗号文

SgScgg2^L2 W2^L2cl

2009/6/11

栗原正純 電気通信大学

14

# RSA暗号

## 暗号文

SgScgg2^L2 W2^L2cl

2009/6/11

栗原正純 電気通信大学

15

# RSA暗号

## 暗号文

SgScgg2^L2 W2^L2cl

2009/6/11

栗原正純 電気通信大学

16

Aさん

2009/6/11

栗原正純 電気通信大学

17

Bさん

2009/6/11

栗原正純 電気通信大学

18

Cさん

2009/6/11

栗原正純 電気通信大学

19

公開通信路

2009/6/11

栗原正純 電気通信大学

20