

「秘密鍵(共通鍵)暗号システム」 と「公開鍵暗号システム」の相違点 説明用資料

2009/06/11作成

2009/6/11

栗原正純 電気通信大学

1

秘密鍵暗号システム

暗号化

2009/6/11

栗原正純 電気通信大学

2

秘密鍵暗号システム

暗号化鍵 = 復号化鍵

2009/6/11

栗原正純 電気通信大学

3

秘密鍵暗号システム

復号化

2009/6/11

栗原正純 電気通信大学

4

秘密鍵暗号システム

暗号化鍵 = 復号化鍵

2009/6/11

栗原正純 電気通信大学

5

公開鍵暗号システム

暗号化。

2009/6/11

栗原正純 電気通信大学

6

公開鍵暗号システム

暗号化鍵_A

2009/6/11

栗原正純 電気通信大学

7

公開鍵暗号システム

暗号化鍵_A

2009/6/11

栗原正純 電気通信大学

8

公開鍵暗号システム

暗号化鍵_A

2009/6/11

栗原正純 電気通信大学

9

公開鍵暗号システム

復号化_B

2009/6/11

栗原正純 電気通信大学

10

公開鍵暗号システム

復号化鍵_B

2009/6/11

栗原正純 電気通信大学

11

秘密鍵暗号システム

ひら文_A

明日の午後1時に図書館に集合

2009/6/11

栗原正純 電気通信大学

12

秘密鍵暗号システム

ひら文_B

明日の午後1時に図書館に集合

2009/6/11

栗原正純 電気通信大学

13

秘密鍵暗号システム

暗号文_A

?xA3!&#Dk\$2uP9%¥)n</p></div><div data-bbox="138 917 213 933" data-label="Text"><p>2009/6/11</p></div><div data-bbox="410 917 584 933" data-label="Text"><p>栗原正純 電気通信大学</p></div><div data-bbox="832 917 859 933" data-label="Text"><p>14</p></div>

秘密鍵暗号システム

暗号文_b

?xA3!&#Dk\$2uP9%¥)n

2009/6/11

栗原正純 電気通信大学

15

秘密鍵暗号システム

暗号文_c

?xA3!&#Dk\$2uP9%¥)n

2009/6/11

栗原正純 電気通信大学

16

公開鍵暗号システム

ひら文_A

明日の午後1時に図書館に集合

2009/6/11

栗原正純 電気通信大学

17

公開鍵暗号システム

ひら文_B

明日の午後1時に図書館に集合

2009/6/11

栗原正純 電気通信大学

18

公開鍵暗号システム

暗号文_A

\$2uP9?x!
k%¥)nA3

2009/6/11

栗原正純 電気通信大学

19

公開鍵暗号システム

暗号文_B

\$2uP9?x!
k%¥)nA3

2009/6/11

栗原正純 電気通信大学

20

公開鍵暗号システム

暗号文。

\$2uP9?x!#Dk%¥)nA3

2009/6/11

栗原正純 電気通信大学

21

Aさん

2009/6/11

栗原正純 電気通信大学

22

Bさん

2009/6/11

栗原正純 電気通信大学

23

Cさん

2009/6/11

栗原正純 電気通信大学

24

公開通信路

2009/6/11

栗原正純 電気通信大学

25

安全な通信路

2009/6/11

栗原正純 電気通信大学

26

Aさん

2009/6/11

栗原正純 電気通信大学

27

Bさん

2009/6/11

栗原正純 電気通信大学

28

Cさん

2009/6/11

栗原正純 電気通信大学

29

公開通信路

2009/6/11

栗原正純 電気通信大学

30