

「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

秘密鍵暗号システム

暗号化

秘密鍵暗号システム

暗号化鍵＝復号化鍵

秘密鍵暗号システム

復号化

秘密鍵暗号システム

暗号化鍵＝復号化鍵

公開鍵暗号システム

暗号化。

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

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

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

秘密鍵暗号システム

暗号文_A

?xA3!&#Dk\$2uP9%¥)n

秘密鍵暗号システム

暗号文_B

?xA3!&#Dk\$2uP9%¥)n

秘密鍵暗号システム

暗号文_c

?xA3!&#Dk\$2uP9%¥)n

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

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

公開鍵暗号システム

暗号文_A

\$2uP9?x!&#Dk%¥)nA3

公開鍵暗号システム

暗号文_B

\$2uP9?x!&#Dk%¥)nA3

公開鍵暗号システム

暗号文_c

\$2uP9?x!&#Dk%¥)nA3

Aさん

Bさん

Cさん

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

Bさん

Cさん

公開通信路