公開鑰匙認證協定 - 簡介



* 公開鑰匙認證協定的特性

◆ 用戶與系統皆必須擁有鑰匙配對(憑證)

- 開放性系統
- 系統安全要求較高的環境。 (K_{RA}, K_{UA})
- 用戶與伺服器較複雜的環境。
- 第一伺服器
 (1) Alice, K_{UB}[R₁]

 (2)R₁, K_{UA}[R₂]

 a

 (3) R₂

 (3) R₂

 (4)

 (5)

 (6)

 (7)

 (8)

 (8)

 (8)

 (8)

 (8)

 (9)

 (1) Alice, K_{UB}[R₁]

 (2)

 (3) R₂
- ◆ 混合型密碼系統(Hybrid Cryptosystem)
 - 資料傳遞效率較高。

多用戶/多伺服器 環境



