

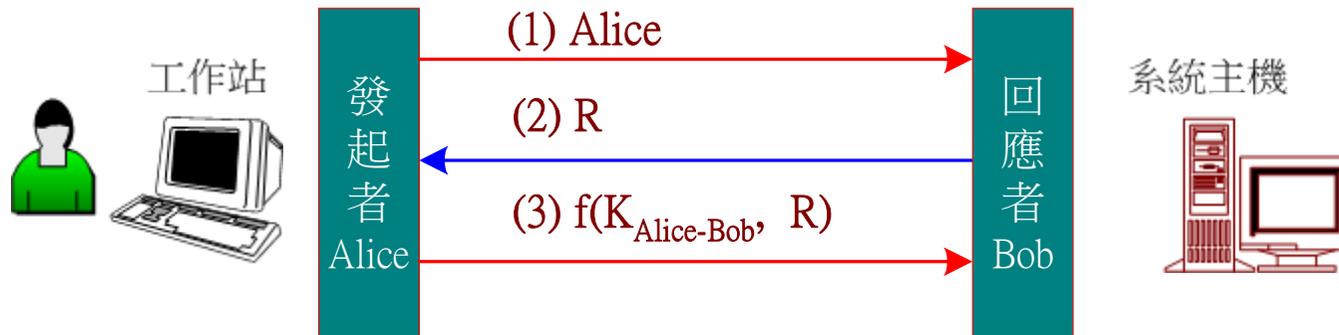
單向共享密鑰認證 - 明文盤問

✿ 單向共享密鑰認證 - 明文盤問

◆ 確認共享密鑰

◆ 偽裝回應者(IP) 騙取加密後密文(採用不可逆加密)。

(a) 明文盤問

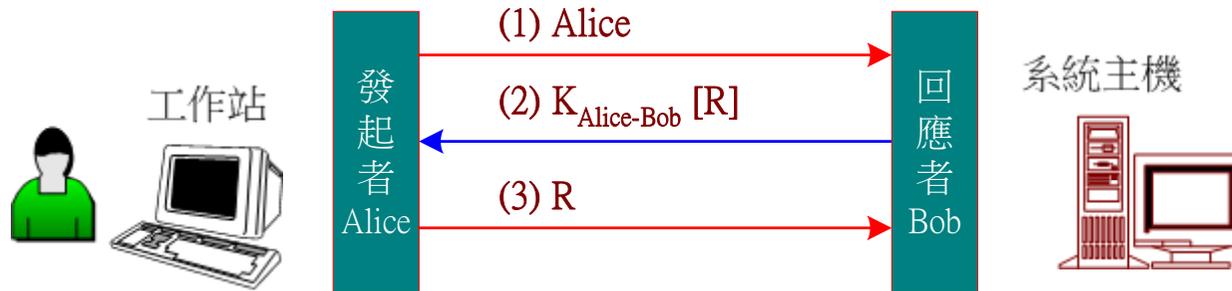


單向共享密鑰認證 - 密文盤問



✿ 單向共享密鑰認證 - 密文盤問

◆ 偽裝發起者騙取密文(可逆性)



單向共享密鑰認證 - 時間戳記



✿ 時間戳記盤問

(a) 加密時間戳記盤問



(b) 雜湊時間戳記盤問

