

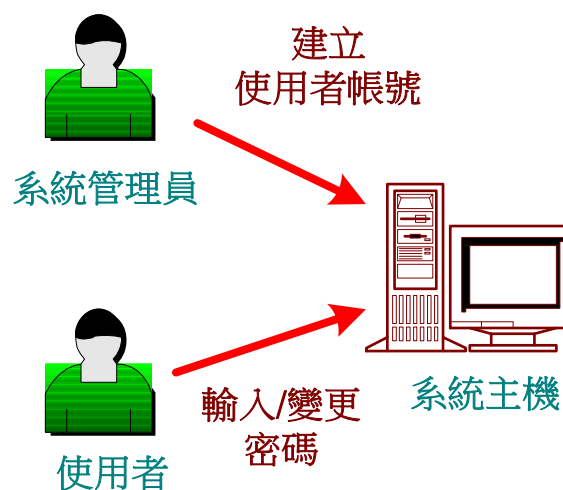
帳號/密碼認證 – 建立密鑰



☀ 共享秘密鑰匙 (Shared Key) 建立

- ◆ 工作站與系統主機之間的共享秘密鑰匙。
- ◆ 『醃製法』 (Salt Value) 加密鑰匙。
- ◆ 處理過程：

- 密碼 (Password) : P
- 個人的鹽 : S_m , $m = 1, 2, \dots, n$
- 演算法 : $f()$, DES、MD5、RC4
- 個人的共享密鑰 : $K_T = f(P, S_m)$



名稱	鹽	共享密鑰
Alice	451	$f(P_A, 451)$
Bob	789	$f(P_B, 789)$
Trudy	267	$f(P_T, 267)$
.....