Esercizio 2

I processi A e B dispongono soltanto di un cifrario a chiave pubblica e di uno a chiave simmetrica. Si assuma che A conosca Π_B, la chiave pubblica di B, e viceversa. Supponendo che i clock non siano sincronizzati, progettare un protocollo di distribuzione delle chiavi che soddisfi i seguenti requisiti:

1. al termine dell'esecuzione del protocollo, il processo A ha la prova che il processo B dispone della chiave di sessione e viceversa;
2. il protocollo è resistente ad attacchi di replay;
3. la chiave di sessione è generata da uno dei due processi.

Modificare il protocollo assumendo che entrambi i processi contribuiscano alla generazione della chiave di sessione come segue: il processo A genera la quantità K_A, il processo B la quantità K_B e la chiave di sessione e' data da $K_{AB} = f(K_A, K_B)$.

Soluzione

Protocollo 1.

$M1 \quad A \rightarrow B: \quad \{K_a\}_{\Pi_b}$

$M2 \quad B \rightarrow A: \quad \{K_a, K_{ab}\}_{\Pi_a}$

$M3 \quad A \rightarrow B: \quad \{A, B\}_{k_{ab}}$

Protocollo 2

$M1 \quad A \rightarrow B: \quad \{K_a\}_{\Pi_b}$

$M2 \quad B \rightarrow A: \quad \{K_a, K_b\}_{\Pi_a}$

$M3 \quad A \rightarrow B: \quad \{K_b, K_a\}_{\Pi_b}$

$M4 \quad B \rightarrow A: \quad \{A, B\}_{K_{ab}}$

$M5 \quad A \rightarrow B: \quad \{B, A\}_{K_{ab}}$