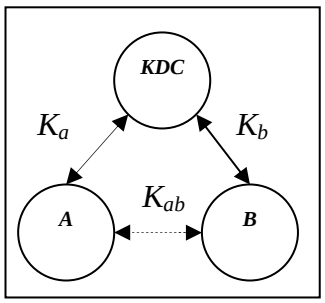
Esercizio 2

A e *B* devono stabilire una chiave di sessione K_{ab} da utilizzare con un cifrario (E, D). A tale scopo *A* e *B* utilizzano il protocollo di Diffie-Hellman (DH), con parametri pubblici *p* e *g*. Per evitare l'attacco dell'uomo nel mezzo, il protocollo DH viene esteso per mezzo di un Key Distribution Center (KDC), on-line, con cui *A* e *B* condividono una chiave simmetrica, rispettivamente, K_a e K_b.



Quesito 1. Progettare il protocollo DH-esteso (E-DHP) in modo che soddisfi i seguenti requisiti: a) il protocollo non è soggetto all'uomo nel mezzo; b) al termine del protocollo, *A* ha la prova che *B* dispone di K_{ab} e viceversa.

Quesito 2. Valutare se nell'interazione tra *A, B* e *KDC* è possibile sostituire il cifrario (*E, D*) con un *message authetication code* $h_K()$.

Quesito 3. Si assuma che un avversario disponga di una Kab passata ed abbia registrato tutti i messaggi che hanno portato a stabilirla. Tramite un replay attack, l'avversario può indurre A (o B) a stabilire ancora Kab come chiave condivisa? Motivare la risposta.

Soluzione

Quesito 1.

A -> KDC: A, B, {A, B, Xa}Ka
KDC->A: A, B, {A, B, Xa}Kb
B -> KDC: B, A, {B, A, Xb}Kb
KDC->A: B, A, {B, A, Xb}Ka
A->B: {A}Kab
B->A: {B}Kab

Quesito 2

{Z}Kx può essere sostituito con hKx(Z)

Quesito 3. No, l'avversario non può indurre A (o B) a stabilire ancora Kab. Infatti il protocollo DH richiede che ad ogni istanza di esecuzione, ciascuno dei peer generi una nuova chiave segreta in modo random. Per cui, anche se l'avversario riusa Xb, A genererà una nuova chiave segreta a' e perciò l'a nuova chiave sarebbe kba'. Per poter stabilire tale chiave l'avversario dovrebbe ricavare b da Xb ma ció richiede di risolver il DLP.