Laurea Specialistica in Ingegneria Informatica
SICUREZZA NELLE RETI
Appello del 08 luglio 2011

Nome e Cognome _____ **Matricola** _____

ESERCIZIO 1 punti:16

Con proprietà di linguaggio e precisione matematica, il candidato i) specifichi il protocollo di Diffie-Hellman; e ii) ne argomenti la sicurezza rispetto ad un avversario passivo. Inoltre, iii) estenda il protocollo DH al caso di *n* processi(Group-DH), iv) valutandone la complessità in termini di numero e dimensione dei messaggi trasmessi.

ESERCIZIO 2 punti: 6

Alice e Bob utilizzano il protocollo Diffie-Hellman (DH) per stabilire una chiave di sessione. Al fine di evitare l'attacco dell'uomo-nel-mezzo, Alice e Bob mantengono un segreto condiviso a-priori σ. Progettare e verificare con la logica BAN un protocollo il protocollo DH-modificato che utilizza tale segreto. La verifica può dirsi conclusa con successo quando si raggiungono i beliefs $B \mid\equiv \overset{\nu}{\mapsto}$ e $A \mid\equiv \overset{\nu}{\mapsto}$, con X_A ed X_B parametri pubblici di Alice e Bob, rispettivamente.

ESERCIZIO 3 punti:8

Con proprietà di linguaggio e precisione matematica, il candidato spieghi il problema del *keystream reuse* in WEP.

Laurea Specialistica in Ingegneria Informatica

SICUREZZA NELLE RETI

Appello del 19 febbraio 2009

Soluzione

ESERCIZIO 1

Vedi appunti.

ESERCIZIO 2

M1 $A \rightarrow \quad n_A$

M2 $B \rightarrow \quad n_B$

M3 $A \rightarrow \quad {}_A, h_\sigma$ ‘ v ||

M4 $B \rightarrow \quad {}_B, h_\sigma$ ‘ v ||

IPOTESI

1. $A \mid\equiv \overset{v}{\mapsto}$, $B \mid\equiv \overset{v}{\mapsto}$
2. $B \mid\equiv \overset{-}{\rightleftharpoons}$, $A \mid\equiv \overset{-}{\rightleftharpoons}$
3. $A \mid\equiv$, $B \mid\equiv$
4. $A \mid\equiv \Rightarrow \overset{v}{\mapsto}$, $B \mid\equiv \Rightarrow \overset{v}{\mapsto}$

PROTOCOLLO IDEALIZZATO

M3 $A \rightarrow \quad / \overset{v}{\mapsto} \backslash \rangle / \backslash / \sigma$

M4 $B \rightarrow \quad / \overset{v}{\mapsto} \backslash \rangle / \backslash / \sigma$

TESI

1. $B \mid\equiv \overset{v}{\mapsto}$, $A \mid\equiv \overset{v}{\mapsto}$

ESERCIZIO 3

Vedi appunti.