Appello del 13 settembre 2011

NOME E COGNOME _____ **MATRICOLA** _____

ESERCIZIO 1 punti:10

Con proprietà di linguaggio e precisione matematica, il candidato i) descriva il protocollo *one-time pad* (OTP); ii) elenchi le ipotesi sotto le quali OTP è un cifrario ideale e ne discuta le implicazioni pratiche.

ESERCIZIO 2 punti: 10

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 con un Key Distribution Center (KDC). Siano σ_A e σ_B i segreti di Alice e Bob rispettivamente. Supponendo che i clock siano sincronizzati, progettare e verificare con la logica BAN un protocollo DH-modificato che permette ad Alice e Bob di stabilire una chiave di sessione utilizzando il KDC. La verifica può dirsi conclusa con successo quando si raggiungono i beliefs $B \mid\equiv \overset{X_A}{\mapsto} A$ e $A \mid\equiv \overset{X_B}{\mapsto} B$, con X_A ed X_B parametri pubblici del protocollo DH di Alice e Bob, rispettivamente.

ESERCIZIO 3 punti:10

Con proprietà di linguaggio e precisione matematica, il candidato spieghi la vulnerabilità del protocollo di autenticazione di WEP.

Appello del 13 settembre 2011

NOME E COGNOME _____ **MATRICOLA** _____

Soluzione

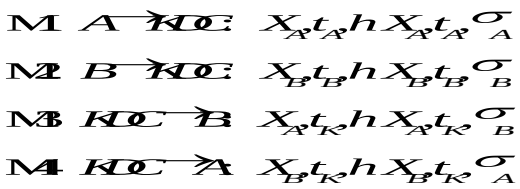
ESERCIZIO 1

Vedi appunti.

ESERCIZIO 2

Per ipotesi le quantità σ_A e σ_B sono dei segreti condivisi e, come precisato in sede d'esame, in assenza di ipotesi ulteriori, non possono essere considerati chiavi di cifratura. Ad esempio, con riferimento all'algoritmo DES, un segreto potrebbe essere una *weak-key*. Quello che si può invece ragionevolmente supporre è che il segreto condiviso abbia una dimensione in bit adeguata a contrastare una ricerca esaustiva sebbene questo possa venire a detrimento dell'usabilità. Sulla base di queste considerazioni si può definire il seguente protocollo reale.

PROTOCOLLO REALE



IPOTESI

1. $A \models \overset{X_A}{\mapsto} A, B \models \overset{X_B}{\mapsto} B$
2. $A, K_{AC} \models \overset{\sigma_A}{\leftrightarrow} C, \; B, K_{BC} \models \overset{\sigma_B}{\leftrightarrow} C$
3. $A, K_{AC} \models \#(t_A), \; B, K_{BC} \models \#(t_B), \; A, B, K_{AB} \models \#(t_K)$
4. $A \models B \overset{X_B}{\Rightarrow} B, \; B \models A \overset{X_A}{\Rightarrow} A$
5. $A \models K_{AC} \overset{X_B}{\Rightarrow} B, \; B \models K_{BC} \overset{X_A}{\Rightarrow} A$

PROTOCOLLO IDEALIZZATO

$$\text{M1} \quad A \rightarrow KDC: \quad \left\langle \overset{X_A}{\mapsto} A, t_A \right\rangle_{\sigma_A}$$

$$M2 \quad B \rightarrow KDC \quad \left\langle \overset{X_B}{\mapsto} B, t_B \right\rangle_{\sigma_B}$$

$$M3 \quad KDC \rightarrow B \quad \left\langle A \overset{\equiv}{\mid} \overset{X_A}{\mapsto} A, t_K \right\rangle_{\sigma_B}$$

$$\text{M4} \quad KDC \rightarrow A: \quad \left\langle B \overset{\equiv}{\mid} \overset{X_B}{\mapsto} B, t_K \right\rangle_{\sigma_A}$$

DIMOSTRAZIONE (SKETCH)

Alla ricezione del messaggio M1, per le ipotesi 2 e 3, $KDC \overset{\equiv}{\mid} A \overset{\equiv}{\mid} \overset{X_A}{\mapsto} A$. Alla ricezione del messaggio 3, per le ipotesi 2, 3, 4, 5, $B \overset{\equiv}{\mid} \overset{X_A}{\mapsto} A$. Un ragionamento analogo può essere fatto per i messaggi M2 e M4. Si ottiene quindi $B \overset{\equiv}{\mid} \overset{X_A}{\mapsto} A, A \overset{\equiv}{\mid} \overset{X_B}{\mapsto} B$

ESERCIZIO 3

Vedi appunti.