Sicurezza nelle reti e nei sistemi informatici – 13/9/2011
Tempo: 100 minuti. N.B.: le domande potrebbero avere pesi differenti!

1. Hashing

a. Definire i concetti di funzione di hash crittografica e di resistenza alle collisioni (debole e forte). Spiegare cosa è, discutendone le conseguenze pratiche, un "birthday attack" ("attacco del compleanno").
b. Data una funzione di hash che mappa stringhe di m bit in stringhe di n bit ($m \gg n$), discutere come ottenere lo hashing (sempre n bit) di un messaggio di M bit, con $M \gg m$.
c. Illustrare infine gli usi principali delle funzioni hash in crittografia.

2. Password

a. Descrivere cosa è un attacco offline alle password. È necessario che l'attaccante sia in possesso di qualche informazione affinché l'attacco abbia senso?
b. Descrivere lo schema EKE e spiegare come esso possa essere modificato per ottenere la cosiddetta "augmented property" (l'autenticatore conosce una informazione derivata dalla password che può essere usata per la verifica della password stessa, ma chi si autentica deve conoscere la password). È vulnerabile ad attacchi offline alle password? Spiegare.

3. Firma digitale e confidenzialità

Con riferimento a RSA e al metodo di firma con RSA "puro" (in cui si codifica con chiave privata il documento da firmare) rispondere alle seguenti domande:

a. Usando il metodo RSA puro per firmare due documenti identici, le firme sono identiche?
b. Dati due documenti X e Y e le corrispondenti firme s(X) e s(Y) (create usando la stessa chiave RSA) individuare un terzo documento Z (anche senza senso compiuto) e la corrispondente firma s(Z).
c. Discutere come lo standard PKCS permette di risolvere i problemi evidenziati in precedenza.

4. Gioco "trova il centro"

Alice, Bob e Charlie giocano a "trova il centro", che consiste nello scegliere un intero positivo da un intervallo prestabilito: vince chi ha scelto il valore intermedio. Se due o tre valori sono eguali la partita è patta.
I tre giocano con il seguente protocollo, in cui K_A e K_B sono chiavi (per crittografia simmetrica) di A e B; a, b, e c sono gli interi scelti da A, B e C; N è il massimo intero ammissibile.

$A \rightarrow B$: (A, B, C, N, $K_A(a)$)	{ A propone a B una partita fra A, B e C, indica il max N ed invia la cifratura della sua scelta a fatta tramite K_A }
$B \rightarrow C$: (B, C, A, N, $K_A(a)$, $K_B(b)$)	{ B invia a C, il max N, la scelta di A (cifrata) e la propria scelta (cifrata) }
$C \rightarrow A$: (C, A, B, $K_B(b)$, c)	{ C invia ad A la scelta di B (cifrata) e la propria scelta (in chiaro) }
$A \rightarrow B$: (A, B, C, K_A, c)	{ A invia a B la propria chiave di cifratura e la scelta di C in chiaro; ora B può conoscere i tre valori }
$B \rightarrow C$: (B. C, A, K_A, K_B)	{ B invia a C le chiavi di A e B: ora C può conoscere i tre valori }
$C \rightarrow A$: (C, A, B, K_B)	{ C invia ad A la chiave di B; ora A può conoscere i tre valori }

a. Analizzare la robustezza del protocollo rispetto possibili comportamenti fraudolenti da parte dei giocatori.
b. Modificare il protocollo (senza snaturarlo) per eliminare le vulnerabilità individuate.

5. Domande brevi (al più 8 linee e una figura per risposta)

a. Descrivere sommariamente quali garanzie di sicurezza e quali limitazioni derivano dall'adozione di una infrastruttura basata su Kerberos.
b. Descrivere la fase di autentica in SSL e discuterne la sicurezza.