Sicurezza nelle reti e nei sistemi informatici – 7/7/2011
Tempo: 100 minuti. N.B.: le domande potrebbero avere pesi differenti!

1. Cifrari a blocchi e modi di operazione

a. Descrivere in dettaglio un modo di operazione che consente di eseguire una cifratura simile a quella dei cifrari a flusso sincroni, analizzando anche la sua resistenza agli errori e la sua parallelizzabilità in cifratura e decifratura.
b. Definire il concetto di *cifrario perfetto* e discutere la possibilità che la cifratura a blocchi di cui al punto precedente possa costituire una cifratura perfetta.

2. Campi finiti e AES

a. Definire il campo finito $GF(2^4)$, illustrarne le proprietà principali e spiegare come mossa essere realizzata la sua aritmetica (addizione e moltiplicazione) in termini di polinomi su campi finiti.
b. Descrivere sinteticamente lo standard di cifratura simmetrica AES e spiegare in quale/i fase/i faccia uso dell'aritmetica sui campi finiti.

3. Firma digitale

a. Descrivere lo standard di firma DSA, spiegando in dettaglio come viene calcolata la firma e come se ne possa fare la verifica.
b. Discutere il ruolo del numero casuale k usato nella firma e spiegare quali vulnerabilità verrebbero introdotte nel caso di una sua "inadeguata" gestione. Che potere avrebbe un avversario in possesso di k?

4. Gioco "indovina il risultato"

a. Alice e Bob debbono lanciare un dado (uno a testa) e prima di farlo scommettono sul risultato che si otterrà (somma dei due valori). Vince chi indovina il risultato. I due giocano con il seguente protocollo.
{ A lancia il dado ottenendo a; sceglie la sua previsione del risultato V_A, genera un nonce r_A }
A → B: (A, $r_A(a)$, V_A) { $r_A(a)$ è la cifratura di a usando la chiave simmetrica r_A }
{ B lancia il dado ottenendo b; sceglie la sua previsione V_B, genera un nonce r_B }
B → A: (A, $r_B(b)$, V_B) { $r_B(b)$ è la cifratura di b usando la chiave simmetrica r_B }
A → B: (A, r_A)
{ B decifra $r_A(a)$ ed ottiene a, calcola la somma a+b e verifica se c'è un vincitore }
B → A: (B, r_B)
{ A decifra $r_B(b)$ ed ottiene b, calcola la somma a+b e verifica se c'è un vincitore }
Si richiedere di discutere la sicurezza del protocollo rispetto a possibili comportamenti malevoli di Alice e/o Bob.
b. Introdurre piccole modifiche nel protocollo per eliminare le vulnerabilità individuate al punto precedente.

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

a. Descrivere sommariamente le caratteristiche fondamentali del protocollo SSH in termini di architettura protocollare e di servizi resi agli utenti.
b. Descrivere informalmente le regole di filtraggio pacchetti ritenute idonee in un firewall personale che consenta l'accesso dall'esterno solamente ai servizi di stampa CUPS (protocollo HTTP, porta 631) e all'SSH daemon (porta 22). Naturalmente dovrebbero essere consentite tutte le comunicazioni da/per localhost.