Sicurezza dei Sistemi Informatici
Prof. Stefano Paraboschi
Prova in itinere del 30/4/2014

A. Si vuole realizzare un servizio di recupero di chiavi di cifratura. La chiave K da proteggere ha una dimensione pari a 120 bit. Si vuole che la chiave sia recuperabile con la collaborazione degli utenti A, B e C. Si considerino queste due alternative:

   1. Si creano 2 sequenze casuali di 120 bit, $S1$ e $S2$. Si assegna $S1$ ad A, $S2$ a B e il risultato di $S1 \oplus S2 \oplus K$ a C.
   2. Si assegnano ad A i primi 40 bit della chiave, a B i bit dal 41-esimo all'80-esimo e a C gli ultimi 40 bit.

   Si confrontino le due soluzioni dal punto di vista della sicurezza.

B. Si consideri la costruzione di un MAC mediante l'applicazione di una cifratura con modo CBC con cifrario AES con chiave k nota. Il risultato della funzione hash è rappresentato dal valore dell'ultimo blocco cifrato. Si analizzi sinteticamente il comportamento di questa funzione dal punto di vista dell'efficienza e della sicurezza. Si illustri brevemente se la ricerca di una collisione per questa funzione é ancora suscettibile all'attacco del compleanno.

C. La tecnica di Diffie-Hellman puó essere usata per realizzare un crittosistema a chiave pubblica. Il sistema sceglie i valori p e g e ciascun utente mostra come chiave pubblica il valore g^{k_p}. Descrivere i principi di funzionamento della tenica Diffie-Hellman che verrebbero utilizzati in questo contesto. Mostrare come Alice e Bob potrebbero dialogare in modo sicuro (si trascurino i rischi di attacchi replay e si assuma che sia Alice sia Bob conoscano con certezza il valore g^k dell'altro).