ESERCIZIO DI SICUREZZA [6 PUNTI]

Quesito 1. Il candidato dia la definizione delle proprietà *preimage resistance*, *second-preimage resistance* e *collision-resistance* di una funzione hash.

Le funzioni hash sono utilizzate nelle *one-time password* (OTP), una tecnica che permette ad un utente di identificarsi ad un server attraverso un terminale inaffidabile.

Setup

1. L'utente U sceglie un numero random segreto s.
2. L'utente calcola $n+1$ password come segue: $P_n = h(s)$, $P_{n-1} = h(P_n) = h^2(s)$, …, $P_1 = h(P_2) = h^n(s)$, $P_0 = h(P_1) = h^{n+1}(s)$.
3. L'utente distribuisce la password P_0 al server S con metodi off-line in modo però da garantirne l'autenticità.

Utilizzo

1. Alla i-esima identificazione, $1 \leq i \leq n$, l'utente si identifica inviando al server S la password P_i.
2. Alla ricezione di P_i, il server verifica se $P_{i-1} = h(P_i)$. In tal caso l'identificazione ha esito positivo; negativo altrimenti.

Quesito 2. Il candidato indichi, motivando la risposta, di quali proprietà è sufficiente che goda la funzione hash h per un utilizzo in uno schema OTP.

Quesito 3. Il candidato indichi, motivando la risposta, quale tipo di avversario (attivo o passivo) uno schema OTP permette di contrastare.

SOLUZIONE

Quesito 1.
La risposta e' nel lucido 10 del blocco di lucidi relativo alle funzioni hash (http://www2.ing.unipi.it/~d8333/Teaching/SeminarioSnR/materiale/Funzioni-Hash.pdf).

Quesito 2.
La funzione deve soddisfare le proprieta' di preimage resistance (*one-way*) e di 2nd-preimage resistance (*weak collision resistance*). Se le proprieta' non fossero soddisfatte, un avversario potrebbe intercettare una password e calcolare tutte le pre-immagini ricostruendo cosi' la catena delle password.

Quesito 3.
OTP permette di contrastare un avversario passivo. Un avversario attivo puo' aggirare OTO con un attacco del tipo *man-in-the-middle*.