Criptografia i Seguretat [104355]

Exercises: Passwords

1. Considerem un sistema de passwords que fa servir passwords d'un màxim de 14 caràcters on cada caràcter pot tenir 32 possibles valors. Si un password té menys de 14 caràcters s'afegeix el caràcter *null* fins arribar a 14 caràcters. El password final amb 14 caràcters és P. Donada una funció hash criptogràfica h considera els següents esquemes:

   Pass1 [1] P es divideix en dues parts de 7 caràcters X, Y. El password es guarda com $(h(X), h(Y))$. No es fa servir *salt*.

   Pass2 P es guarda com $h(P)$. No es fa servir *salt*.

   1. Quin esquema és més segur? Per què?
   2. En l'esquema **Pass1** es podria donar que un password de 10 caràcters fos menys segur que un de 7?

2. Suposem que tenim un sistema de passwords on cada password és de 8 caràcters i cada caràcter pot tenir 128 valors. El sistema té un fitxer amb passwords resumits amb alguna mena d'esquema basat en funcions hash que conté 2^{10} passwords diferents.

   Un atacant, Eva, té un diccionari amb 2^{20} passwords comuns, i la probabilitat que un password qualsevol estigui al diccionari és d'$1/4$. Assumim que el cost de pre-computar passwords és extremament costós i per tant no es pot fer. Si no es diu el contrari assumim també que el sistema no fa servir *salt*.

   Per aquest cas concret mesurem el cost en nombre de computacions de hashos de passwords. A més, mesurarem sempre el cost mig (no el pitjor cas).

   1. Eva vol trobar el password de *root* sense fer servir el diccionari. Quin atac farà? Quin cost tindrà? I si el sistema fa servir *salt*?
   2. Ara Eva, vol trobar el password de *root* però sí que fa servir el seu diccionari. Quin atac farà? Quin cost total tindrà trobar el password?
   3. Eva vol trobar qualsevol password del fitxer de passwords, sense fer servir el seu diccionari. Quin cost té aquest atac? Sense haver de tornar a calcular el cost indica quines implicacions tindria l'ús de salt.

3. Implementeu les funcions Pass1 i Pass2 fent servir *Python hash()*.

[1] Aquest esquema equival a LM hash, que fa servir LAN Manager de Windows (actualment no es fa servir).