HOMEWORK SET 1

1. Per ciascuno dei quattro tipi di meccanismo per il controllo degli accessi
   - **per-subject access control list** (cioè, una lista per ciasun subject con tutti gli oggetti e relative permessi concessi al subject)
   - **per-object access control list** (cioè, una lista per ciasun object con tutti i soggetti che hanno accesso a quell'oggetto)
   - **access control matrix**
   - **capability** (token individuali – uno per ciascuna terna **(subject,permesso,object)**)

   spiegare (descrivendo uno schema di un algoritmo) le difficoltà (computazionali) per

   a) stabilire chi è autorizzato ad accedere ad un determinato oggetto durante l'esecuzione
   b) aggiungere l'accesso ad uno specifico insieme di oggetti per un nuovo soggetto
   c) rimuovere l'accesso ad un oggetto specifico da parte di un particolare soggetto
   d) creare un nuovo oggetto al quale tutti I soggetti hanno accesso per default.

2. Representare le etichette di sicurezza usando la notazione

   <*security level*; *set of categories*>.

I **security levels** sono **(top secret, secret, confidential)** in ordine decrescente, e l'insieme di tutte le **categorie** è {cat, cow, dog, moose, pig}. Può un utente con etichetta <*secret; { dog, cat, pig }*> avere accesso in lettura, scrittura od entrambi a documenti classificati in ciascuno dei seguenti modi ?

   a) <*top secret; { dog }*>
   b) <*secret; { dog }*>
   c) <*secret; { dog, cow }*>
   d) <*secret; { moose }*>
   e) <*confidential; { dog, pig, cat }*>

3. Dimostrare che le "enforcement rules" del modello di Clark-Wilson possono simulare il modello di Biba.

4. Un utente vuole editare il file **xyzzy** in un sistema basato su 'capability'. Come può l'utente essere sicuro che l'editore non può accedere altri file? Può essere fatto in un sistema basato su ACL? Come, oppure perchè non si può fare?

5. Nel modello Chinese Wall, sia S l'insieme dei soggetti, O l'insieme degli oggetti, e l_1:$O \rightarrow C$ e l_2: $O \rightarrow D$ le funzioni che associano a ciascun oggetto la classe in C dei conflitti di interesse (COI) e l'insieme in D dei dati della compagnia (CD), rispettivamente. Il valore nella matrice 'storica' di accesso per il soggetto $s \in S$ e l'oggetto $o \in O$ si denota con $H(s, o)$ ed ha valore *true* se il soggetto *s* ha, od ha avuto, accesso 'read' all'oggetto *o*, ed ha valore *false* altrimenti. (Notare che *H* NON è una 'access control matrix', perché non indica gli accessi permessi ma solo gli accessi richiesti.) Sviluppare un algoritmo che genera una 'access control matrix' *A* a partire dalla matrice 'storica' *H* del Chinese Wall Model.

6. Nello schema a soglia di Shamir, sono forniti 3 punti (‘shadows’) con valori (2, 123), (4, 345) e (5, 378). Trovare il polinomio ed il segreto, ipotizzando che la soglia sia 3 e l’aritmetica è svolta in GF(787) (cioè, modulo 787).

7. Un medico ‘tossicodipendente’ da analgesici può prescrivere una ricetta per se stesso. Dimostrare come RBAC in generale e specificatamente la definizione di ‘separation of duty’ può essere usato per gestire il rilascio di medicine ed impedire che un medico prescriva medicine a se stesso.

8. Elencare l’origine e la destinazione del flusso di informazione in ciascuna delle seguenti istruzioni:

a) `sum := a + b + c;`

b) `if a + b < c + d then q := 0 else q := 1;`

c) `write( a, fileOut );`

d) `read( x, fileIn );`

e)
```
case (k) of
        0:    d := 10;
        1 , 2:  d := 20;
        other: d := 30;
end; /*case*/
```

f) `for i := min to max do k := 2 * k + 1;`

g)
```
repeat
        a[i] := 0;
        i  :=  i - 1;
until i <= 0;
```