Homework 4

Due Date : March 17, 1999 **Points** : 200

1. (*20 points*) A computer security expert claims that cryptography is all that is necessary to provide network security. Explain why this is false; in particular, explain why encryption protocols do not provide adequate protection in the absence of trusted hosts.
2. (*30 points*)Following the approach we used in class, give security conditions for the **case** statement:

```
case a of
      v1: S1;
      v2: S2;
      .
      .
      .
      vn: Sn;
end;
```

3. (*40 points*)Assume objects are statically bound to security classes.
   a. For the following program, illustrate the compile-time certification checks:

```
program p1(k, m, f, g, h)
var k: file class K;
m: file class M;
f: file class F;
g: file class G;
h: file class H;
a: integer class A;
b: integer class B;
begin
      input a from f;
      input b from g;
      while b ≠ 0 do
      begin
            if a > 0 then output b to h;
            if b > 0 then output a - b + 1 to k;
            output b to m;
            input a from f;
            input b from g;
      end
end.
```

   b. The following partial orders define 2 lattices:

   L_1: C ≤ S

   L_2: $D_0 \subseteq D_1 \subseteq D_3$, $D_0 \subseteq D_2 \subseteq D_3$

   Assume a lattice of security classes constructed from the cross-product of L_1 and L_2 and determine the security of the program in part a if:

A = (S, D_3)	B = (C, D_1)	F = (S, D_2)
G = (C, D_1)	H = K = (S, D_3)	M = (C, D_3)

4. (*60 points*) Consider the intrusion detection system model, which consists of sensor mechanisms, analysis engines, and notification engines. Please generalize this model to cover all system auditing mechanisms.
5. (*50 points*) The program *lsu* is a version of *su* that uses an access control file and the user's password to give access to shared accounts. It runs setuid to *root* on UNIX systems. On the web page is a tarball of the program *lsu.tar*. Download it and find at least 2 potential security vulnerabilities. You do ***not*** need to exploit it, but you must say how you could exploit it.