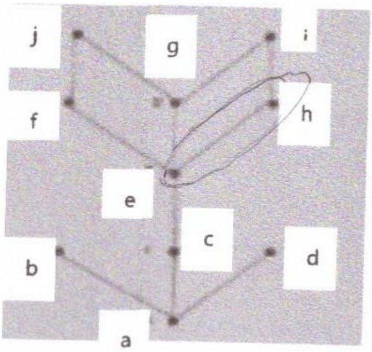
1. (10point) An internet café has asked you to evaluate their security. Outline the threat model you will use.

2. (5point) Given two objects at different security levels h, e, what is the minimal security level a subject must have to be allowed to read both objects?



3. (5point) In a hospital we have 4 kinds of users: Doctor, Nurse, Secretary, Patient. In this hierarchy, Doctors are superior to Nurse, Secretary, and Patient. Nurse and Secretary are superior to Patient, but Nurse is neither superior nor inferior to Secretary. Medical information have several security levels for files, in decreasing order: Operating Room, Emergency, and Personal. Draw a lattice of all the security clearances.

4. (5point) Suppose that a **Recipient** (containing payment information) has security level (secretary, Personal), a **Prescription** for antibiotics has security level (Doctor, Emergency), the **List** of medical tools necessary for an operation has security level (Nurse, Operating room) and the **File** containing the home address of patients in the hospital has security level (Secretary, Emergency). Place all these documents (in bold in the paragraph above) on the preceeding lattice.

5. Suppose that **Dave** the surgeon has clearance (Doctor, Operating room), **Nancy** the nurse has clearance (Nurse, Emergency), **Shari** the secretary has clearance (Secretary, Emergency) and **Paul** the patient has clearance (Patient, Personal). In the Bell-Lapadula model, say if the following actions are allowed, explaining each time why that is:

a) Dave writes on the LIST

b) Nancy reads the File

c) Paul Writes on the Prescription

d) Shari reads the Receipt

6. (5 points) Why are definitions and proofs important? Why "security through obscurity" is not a good idea?

7. (15 points) Security Proof

(i) (5 points) Give the **FORMAL** definition of the notion of OW-CPA security.

(ii) (10 points) We remind the definition of a one-way function: a function f is a one-way function if, for a randomly chosen x in the domain of f, no polynomial-time algorithm can compute x when given only the description of f and $f(x)$. We define the encryption algorithm E, which has a one-way function as its public key, as follows:

- sample a random x in the domain of f.
- output $<f(x), x \oplus m>$

PROVE that this is a OW-CPA secure encryption scheme if f is a one-way function.

8. (10 points) What is a covert channel? Give an example of a covert channel in Bell-LaPadula and explain why this is a problem.

9. (15 points) Define and explain 'polynomial security' and 'semantic security' (10 points), and show the relationship between these with **diagram** (5 points).

10. (20 points) Write short notes (maximum 100 words) on each of the following topics.

(i) ISO 27001 Information Security Management System (10 points)

(ii) In what way is the encryption scheme known as DES considered weak? (10 points)