Q1.

a) (Classified, {Army, Navy}) **dominates** (Unclassified, {})
b) (Top Secret, {Army, Air}) **not dominates** (Secret, {Army, Navy})
c) (Secret, {Army, Navy, Air}) **dominates** (Secret, {Air, Navy})
d) (Secret, {Navy, Army}) **not dominates** (Top Secret, {Army, Navy})

Q2.

- OCSP is standard IP which is used to obtain certificate revocation status of the public key digital certificate without having to download the entire CRL (Certificate revocation list).
- We have OSCP responders which responds to the requestor with the status of the certificate which is in the format – general, revoked or unknown.
- In the older approach, the entire CRL had to be downloaded. This had a maximum of 512 entries. The list may get updated in certain interval and we need to download it again to check for the validity of the certificate.

Advantages of OCSP:

- Immediate revocation of the certificate – The validity of the certificate will be voided immediately after it is reported. Users can report if their certificate/keys have been stolen.
- Saves a lot of overhead – In CRL, client must search through the revocation list. This can be 1000's of lines. Instead client can query the status of the single certificate rather than downloading and processing the entire list.
- Does not require additional memory – No storing of revocation list required.

Disadvantages of OCSP:

- Internet connection is required all the time. While CRLs can work without internet as well since they use cached data. Requires the server to be up all the time.
- Slower – OCSP requires time to obtain revocation status from the external server.
- Vulnerable to replay attacks – The signed response from OCSP server can be captured and replayed to the requester even after the validity is revoked.
- Privacy issues – It requires contacting the third party for the certificate validation.

Q3.

- Concept- Magnetic strip will be changed to the following:
  - Account number of C – AcNr (C)
  - Pin of M – E_B (PIN (M))
- So Now the card is modified to have a different pin with the same account number. The attack can be performed in the following way
  - The ATM scans the magnetic strip and thinks it is of customer C. Since account number is of C. This is a valid number.
  - When prompted to enter the pin, M enters his pin. This is then matched with that of the card. This will be in this format – E_B (PIN (M)) matches with that on the card.
  - Now, M can easily withdraw money from C’s account.