Group A [3 + 2 + 2 + 3 marks]

1. Explain the write access property of BLP model. Also state the advantage of enforcing this property.
2. What is the key advantage of IPsec AH over ESP?
3. What are the key drivers or motivations behind the use of an IDS.
4. Why should a business invest in a UTM firewall? Also list any four modules that could be included in it.

[3 + 3 + 2 + 2 marks] **Group B**

1. Compared to Biba model, what additional protections of integrity are provided in Clark Wilson model?
2. Briefly describe the process of deriving the master key in TLS handshake.
3. Discuss the requirements for a signature-based IDS to be effective?
4. Briefly discus the statement: Application-level gateway is the very powerful kind of firewall.

Group A

Q1

Can only write to the same level as subject's clearance, or to a higher level (append mode). Writing to lower levels in not allowed, since this action can potentially leak sensitive information.

Q2

While ESP only protects the payload of IP packet, AH also includes the IP header for authentication check.

Q3

The quicker the attack can be caught and blocked, the lesser the damage will be done. That's why IDS aims to provide real time monitoring.

Q4

To save cost, to reduce the burden of installing & managing separate security products, and to minimize the performance overhead.

Modules: anti malware, intrusion detection, firewall, anti phishing, bandwidth shaping, vpn, web attack scanning

Group B

Q1

Biba mode prevents system modifications by unauthorized users.

CW model goes one step further and also restricts authorized users to make only correct (certified) modifications. Thus, the system always remains in a valid sate of integrity.

Q2

Client and server exchange hello messages sharing each other's random number.

Both securely exchange or establish pre-master key S.

Master key is derived using a function that takes S and both randoms as input.

Q3

- Signatures database should be sufficiently large (covers most known attacks).
- Signatures are continuously updated with the new attack patterns.

Q4

Application-level gateway filters the packets not just on the basis of the headers (IP, port, protocol) but also inspects the packet contents. Thus, it is also able to block packets that contain malware or attack attempts (buffer overflow, sql injection, XSS etc.).