

1. Firewalls

- (a) Explain the terms NAT, DMZ and Bastion host.
- (b) State three advantages and disadvantages of screening routers (packet filters) and Application gateways.

2. Intrusion Detection

Compare and contrast the following:

- (a) Knowledge-based and Behaviour-based Intrusion Detection Systems.
- (b) Host-based and Network-based Intrusion Detection Systems.

3. Cryptography

- (a) Describe what is triple DES? Why is it more secure than single key DES?
- (b) Alice has selected the public key ($n = 33$; $e = 3$). Using this key, Bob sends plaintext X to Alice which encrypts as ciphertext 6. What is the plaintext X ?

4. Authentication

- (a) We know that doing a signature with RSA alone on a long message would be too slow. Suppose we could do division quickly. Would it be reasonable to compute an RSA signature on a long message by first computing what the message equals mod n , for some fixed n and then signing this computed value only. Why or why not?
- (b) Consider an RSA digital signature scheme. Alice tricks Bob into signing messages m_1 and m_2 such that $m = m_1m_2 \pmod n$. Show that Alice can now forge Bob's signature on the message m .

5. Protocols

- (a) Suppose Alice and Bob are using the Diffie-Hellman Key exchange protocol. They choose the public modulo $n = 47$ and the generator $g = 3$. Suppose Alice and Bob secretly choose $x = 8$ and $y = 10$ respectively. What is the secret key they can compute?
- (b) Is the Diffie-Hellman protocol vulnerable against a (wo)man-in-the-middle attack? Explain why or why not.