

## My study guide (Test 1) – Unit 1 – 4

This is an outline study guide for Test 2 (and may change, so please check back). The test accounts for 25% of the module. It is a closed book test, and normal examination conditions apply. A correct answer scores +1, with a negative penalty for an incorrect answer, and a non-answer gets a score of zero.

Area	Notes
Understands the operation of a shifted-alphabet/code shifting encryption.	
Understands the range of asymmetric encryption algorithms.	
Understands the operation of Vigenere encryption algorithms.	
Understands how many encryption keys map to the number of bits in the key.	
Calculates the time to crack a code using brute force, and given specifications.	
Calculates the time to crack a code using brute force, with increasing computing power.	
Understands the difference between stream and block encryption.	
Understands the decryption process in public-key encryption.	
Understands the usage of private keys in authentication.	
Understands how the recipient authenticates the sender.	
Understands the main parameters of a digital certificate.	
Understands the applications which are signed by certificates.	

Understands the operation of the MD5 signature.	
Understands the hash conversion to Base-64.	
Understands key entropy.	
Calculates the exchange parameters for the Diffie-Hellman method.	
Understands the operation of Diffie-Hellman.	
Understands the concept of port scanning.	
Understands the concept of host scanning.	
Understands Snort rules for destination ports.	
Understands Snort rules for source ports.	
Understands the direction of TCP ports.	
Understands how an agent-based system can detect threats.	
Understands the usage of client TCP ports.	
Understands the significance of the three-way handshake for a client-server connection.	
Understand the usage of the three-way handshake for detection of events.	
Understand the usage of TCP flags.	
Understands Labs 1-7.	

**Notes:**

- Questions in total = 35.
- Test times: 9-9:55am or 10-10:55am, Tuesday 1 November 2011, H.5.

**Contact:**

- Prof Bill Buchanan    Email: [w.buchanan@napier.ac.uk](mailto:w.buchanan@napier.ac.uk)
- Richard Macfarlane    Email: [R.Macfarlane@napier.ac.uk](mailto:R.Macfarlane@napier.ac.uk)
- Robert Ludwiniak    Email: [r.ludwiniak@napier.ac.uk](mailto:r.ludwiniak@napier.ac.uk)