Course: Security Engineering **Lecturer: Bruno Crispo**

Written Exam: 15/06/2013
Questions should be answered in English. It's a closed book exam.

Question 1 [1 point]

What are the security properties a cryptographic hash function must satisfy? Provide an example of a use of hash functions.

Question 2 [1 point]

Explain in detail how the RSA algorithm works.

Question 3 [1 point]

3.1. What are the different strategies an organization can adopt to address the identified risk?

3.2. Give an example of operational control, one of technical control and one of management control.

Question 4 [1 point]

Explain in detail how the two modes of operation: Cipher-block chaining (CBC) and Electronic-CodeBook (ECB) work with DES

Question 5 [1 point]

Why a PKI needs a revocation service? What are the motivations to revoke a certificate and who can revoke a certificate?

Question 6 [1 point]

Describe in detail the differences between Tunnel mode and Transport mode in IPsec.

Question 7 [1 point]

What are the techniques that can be used to prevent or mitigate buffer overflow attacks?

Question 8 [1 point]

What is a reference monitor and what is used for? Which security properties a reference monitor must satisfy?

Question 9 [1 point]

Draw the main components of a policy enforcement architecture and explain in details the functionality of each of them.

Question 10 [1 point]

Explain in detail what is a packet-filtering firewall and an application-gateway firewall. What are their main advantages and limitations?