PAPER CODE NO.	EXAMINER : Alexei P Lisitsa
COMP522	DEPARTMENT : Computer Science Tel. No. 0151 795 4250

UNIVERSITY OF LIVERPOOL

First semester examinations 2017/18

PRIVACY AND SECURITY

TIME ALLOWED : Two and a Half Hours

INSTRUCTIONS TO CANDIDATES

Answer FOUR out of FIVE questions.

If you attempt to answer more questions than the required number of questions (in any section), the marks awarded for the excess questions answered will be discarded (starting with your lowest mark).

UNIVERSITY OF LIVERPOOL

Answer **four** out of five questions listed.

1. (a) What are advantages and disadavantges of using stateful packet inspection in firewalls?

(6 marks)

(b) A simple way of finding a collision in a hash function H is as follows

1. Pick initial value I and calculate $H(I)$;

2. Pick randomly further value J an compare $H(J)$ to $H(I)$;

3. Repeat until $H(J) = H(I)$.

Suggest an improvement of this attack, which would likely lead to faster discovery of the collision.

(10 marks)

(c) What are potential problems with the security protection based on the secrecy of an encryption algorithm?

(4 marks)

(d) Explain the following principles of privacy protection specifed in OECD "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data".

- Purpose Specification Principle;
- Openness principle;
- Individual Participation Principle.

(5 marks)

2. (a) Is privacy always protected if only some records of anonymised and aggregated information are known about a person?

(4 marks)

(b) Explain how a hypothetical fast algorithm for integer factorisation can be used to attack RSA encryption.

(9 marks)

(c) What are the main motivations for the legal regulation of cryptography?

(6 marks)

(d) Outline the main steps in the analysis of protocols using epistemic logic.

(6 marks)

3. (a) Define passive security attacks. Explain how the development of quantum cryptography may change the way of dealing with passive attacks.

(6 marks)

(b) Why does one need to combine the methods from two main categories of intrusion detection methods, signature based and anomaly based, to get the best possible protection?

(5 marks)

(c) The following algorithm can be used to compute a hash function. *Generate some public key K for the RSA algorithm. Encrypt M with K and take the last 160 bits of the result as the hash of M.* What is the main disadvantage of this algorithm?

(6 marks)

(d) Describe the RSA-based blind signature technique. Discuss its role in the implementation of electronic payment systems and electronic voting systems.

(8 marks)

4. (a) What is an iteration count in implementations of password-based encryption? How may setting different values to iteration count affect the brute force search attack against the encryption algorithm?

(6 marks)

(b) *Shamir's no-key* protocol shown below can be used to securely establish a key over an open channel. Here p is a publicly known prime number, r_a and r_b are random numbers chosen by A and B, respectively. K is a number chosen by A.

- Message 1. $A \rightarrow B : K^{r_a} \ mod \ p$
- Message 2. $B \rightarrow A : (K^{r_a})^{r_b} \ mod \ p$
- Message 3. $A \rightarrow B : (K^{r_a r_b})^{r_a^{-1}} \ mod \ p$

Explain how B can get access to K. Is the protocol secure against *passive* or *active* attackers? Explain your answer.

(10 marks)

(c) What conclusion can one derive in BAN logic using the *message meaning rule* from the following two assumptions: 1) P believes that it shares a secret key K with Q, and 2) P receives a message containing X encrypted with K?

(5 marks)

(d) For a block cipher, what is the Cipher Feedback Mode (CFB)? What is the purpose of using CFB?

(4 marks)

5. (a) Describe briefly the 4 levels of information protection and the methods used at each level.
(4 marks)

(b) What is the reason for the anonymity protection system *Tor* to use both symmetric and public-key encryption?
(8 marks)

(c) What is a multifactor authentication technique? Give an example and explain the rationale behind it.
(6 marks)

(d) What is Fully Homomorphic Encryption (FHE)? What is the main issue with applications of FHE? Give an example of an application which would benefit from using FHE.
(7 marks)