PAPER CODE NO. **COMP232**	EXAMINER : Alexei Lisitsa DEPARTMENT : Computer Science Tel. No. 0151 795 4250 (office)

UNIVERSITY OF
LIVERPOOL

Second semester examinations 2019/20

CYBERSECURITY

TIME ALLOWED : Open Book Exam

INSTRUCTIONS TO CANDIDATES

Answer all questions

Expected writing time: 2 hours. Please submit your answers as an electronic document in *.pdf, *.doc, or *.docx format. If none of these formats is available in your circumstances you may alternatively submit graphic images of your handwritten answers.

The work must be submitted electronically via Electronic Coursework Submission System (SAM) by 22nd of May, 10.00AM

UNIVERSITY OF LIVERPOOL

1. Explain what are Secure Multi Party Computations and give a detailed example of their possible application. Discuss possible benefits of, and potential issues with your proposed application.

(20 marks)

2. The following algorithm has been proposed to compute a hash function.

Generate some key K for the AES algorithm. Encrypt M with K and take the last 64 bits of the result as the hash of M.

What are the main disadvantages of this algorithm? Can the algorithm be improved by taking the first 64 bits of the result instead of the last 64 bits?

(12 marks)

3. What is a purpose of using multiple layers of encryption in CryptDB approach to querying encrypted databases? Give an example of the situation where using *three* layers of encryption is justified. If needed you may either define some queries in SQL or describe them in the natural language.

(20 marks)

4. The company X has proposed a very fast and reliable biometric unlock system for their smartphones. It recognizes the owner's face with different face expressions, open and closed eyes, etc with very high probability. What are the possible issues of using this system as the only authentication method granting acces to the smartphone?

(8 marks)

5. What could be the purpose of the following protocol, where both parties use RSA public-key algorithm, sk_A is the secret key of A, pk_B is the public key of B, and s is the secret message by B?

- Message 1. $A \to B : \{\{k\}_{sk_A}\}_{pk_B}$;
- Message 2. $B \to A : \{s\}_k$

Explain the rationale behind and the possible issue with this protocol. How can the issue be fixed?

(15 marks)

6. The following schema for password based encryption has been proposed recently.

The password is split into two parts: the first part is short and easy to remember, the second part is randomly generated and kept secret - nobody knows it. When it comes to decryption the user enters his/her first part of the password, and the second secret part is brute-forced by the decryption algorithm and if successful, the ciphertext is decrypted.

Discuss possible advantages and disadvantages of such a schema and compare it with possible alternative solutions.

(25 marks)