University of Dundee

University of Dundee
School of Science and Engineering
Examinations 2017

BSc/MSc Degrees in Computing

AC31012 Information Security

Time allowed: **TWO** hours

Instructions

There are **FOUR** questions.

Candidates must answer **ALL** questions. All questions carry equal marks. Where appropriate, the value of each part of a question is given in square brackets.

Approved calculators may be used in this examination.

Note: This mock exam is based on the 2016 Secure Internet Programming main and resit exams. Questions on material that was not taught in AC31012/AC51042 have been replaced with questions on the new material that was taught this year.

Do not turn over this question paper until instructed to by the Senior Invigilator

1. **(a)** What must be identified and what quantities must be measured in order to perform a security risk assessment? **[6 marks]**

(b) Is it more important to create back-up copies of your private RSA decryption key or back-up copies of your private RSA signing key? Justify your answer. **[6 marks]**

(c) Good sources of randomness are vital for cryptography. Suppose that the implementation of a simple messaging system uses a one-time pad with a flawed random bitstring generator. The generator is seeded with the encryption key obtained from a truly random source, but the flaw in the generator is that it repeats itself after every 10 bytes. You are tasked with decrypting a 2000 bytes long ciphertext generated by this messaging system. You don't have the decryption key, but you know that the plaintext is in English.

How will you attempt to decrypt the ciphertext? **[7 marks]**

(d) Describe 3 possible defences against XSS attacks. **[6 marks]**

2. **(a)** Give an example of a man-in-the-middle attack on a cryptographic protocol. First present the intended message flow for the protocol, then the attack. Finally, state what security property is violated. **[10 marks]**

(b) Alice wants to send an integrity-protected message that authenticates her as the sender of the message to Bob. She chooses to digitally sign her message with DSS.

(i) Which key must Alice use for this purpose? **[2 marks]**

- Alice uses her private key to sign.
- Alice uses her public key to sign.
- Alice uses Bob's public key to sign
- Alice uses Bob's private key to sign

(ii) Which key must Bob use in order to verify Alice's message? **[2 marks]**

- Bob uses his private key to verify.
- Bob uses his public key to verify.
- Bob uses Alice's public key to verify.
- Bob uses Alice's private key to verify.

(c) Political dissidents break into an online public bulletin board. They replace the board's contents with their own propaganda and change all the access credentials so that the administrators are locked out. As a consequence the board is taken offline for a week. What CIA properties are violated by this attack? What CIA properties are not violated? Justify your answer. **[6 marks]**

(d) In a typical authentication protocol the client sends her username and password over an encrypted channel to the server. The server applies a hash function to the received password, looks up the username and compares the hashed password to the hash stored for the user.

(i) Why is there a need to store the passwords as hashes (instead of plaintexts) on the server? After all, the server receives the plaintext password every time the client is authenticating herself. Give two reasons. **[2 marks]**

(ii) Explain why password hashes must be salted. Then explain why salted, SHA-256 hashed passwords may still be vulnerable to attacks.

[3 marks]

3. **(a)** You are setting up a web application with a discussion forum stored in a SQL database on a web server. All communication with the web server is protected by transport layer security (TLS), the web server does not allow insecure HTTP connections.

Discuss for each of the following attacks whether this setup provides any protection against the attack. You may assume that the implementation of the TLS protocol is secure and used properly, that all certificates are correctly verified and no rogue certificates are installed.

[8 marks]

(i) Cross-site scripting (XSS)

(ii) Disclosure of HTTP Basic Authentication Passwords

(iii) SQL injection

(iv) Denial-of service (DOS)

(b) Describe the purpose of digital signature schemes and name one scheme.

[3 marks]

(c) Compute $2^{201} \bmod 3$. **[4 marks]**

(d) Consider the following facts about fictitious people living in the fictitious postal code area DD1 9XZ.

Name	**Age**	**Gender**	**driver's licence**
Alice	32	Female	yes
Vicky	37	Female	no
Claire	28	Female	no
Bob	23	Male	yes
Joan	41	Female	yes
Carl	23	Male	no
Romeo	35	Male	yes
Moe	31	Male	yes
Sam	29	Male	no
John	49	Male	yes

Suppose that the following statistical data is released about the people living in DD1 9XZ:

- There are 4 women and 6 men living in this area.
- 50% of the women have a driver's license.
- 1 in 3 men do not have a driver's license.

(i) Who is in Vicky's anonymity group and what is Vicky's k-anonymity?

[3 marks]

(ii) Who is in Romeo's anonymity group and what is Romeo's k-anonymity?

[3 marks]

(iii) What is the k-anonymity of the released data set? (Give a reason for your answer) **[4 marks]**

4. **(a)** Name and explain 3 differences between Bitcoin and Chaum's offline eCash.

[6 marks]

(b) What security or privacy properties does TOR provide? To what layer of the TCP/IP protocol stack does TOR provide its service? Give a brief explanation of how TOR works. **[6 marks]**

(c) What is the purpose of an initialization vector for stream ciphers? Must the initialization vector be kept secret? Justify your answer.

[4 marks]

(d) Give an example of an encryption scheme that is vulnerable to a chosen plaintext attack. Describe the attack. **[5 marks]**

(e) Suppose you want to log in to `my.dundee.ac.uk`. You access the website over SSL/TLS.

(i) Your browser runs the SSL handshake protocol and receives a certificate chain from the webserver. Why is it important that the browser verifies the entire chain rather than just the X.509 certificate for `my.dundee.ac.uk`?**[2 marks]**

(ii) The certificate signing `my.dundee.ac.uk`'s certificate refers to a server that stores the certificate revocation list. Why is it important to ensure that there are no denial-of-service (DoS) attacks on servers that publish certificate revocation lists?

[2 marks]

END OF PAPER