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 resit exam. Questions on material that was not taught in AC31012/AC51042 have been replaced with questions on material that was taught this year.

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

1. **(a)** Name and define the CIA properties. **[6 marks]**

(b) Alice wants to send a confidential message to Bob. She chooses to encrypt the message with the RSA cryptosystem.

(i) Which of the following keys must Alice use for this purpose? **[2 marks]**

- Alice uses her private key to encrypt the plaintext message.
- Alice uses her public key to encrypt the plaintext message.
- Alice uses Bob's public key to encrypt the plaintext message.
- Alice uses Bob's private key to encrypt the plaintext message.

(ii) Which of the following keys must Bob use in order to read Alice's message? **[2 marks]**

- Bob uses his private key to decrypt the ciphertext.
- Bob uses his public key to decrypt the ciphertext.
- Bob uses Alice's public key to decrypt the ciphertext.
- Bob uses Alice's private key to decrypt the ciphertext.

(c) Describe three differences between public-key encryption schemes and symmetric encryption schemes. **[6 marks]**

(d) What is MD5 and why shouldn't it be used in digital signature schemes? Describe a potential attack. **[9 marks]**

2. **(a)** Explain what XSS attacks are and describe three different types of XSS attacks. **[9 marks]**

(b) You are alerted to the fact that the certificate authority EVE-TRUST has been compromised and may have issued rogue SSL/TLS certificates. EVE-TRUST's root-certificates are installed in every major browser and operating system.

(i) This news reaches you in the middle of an online banking session. You click on the certificate used for your current online banking session and discover that it has been signed by a trustworthy root certificate authority and not by EVE-TRUST.

Barring any unrelated attacks, can you be sure that your present online banking session is secure? Justify your answer. **[3 marks]**

(ii) You operate a web server that only communicates over TLS. Your web server's public key certificate is signed by a trustworthy certificate authority, different from EVE-TRUST. Does the news that EVE-TRUST has been compromised affect the security of the transactions between your webserver and your customers? Justify your answer.

[4 marks]

(c) The use of salt and strong password hashing functions, such as bcrypt or PBKDF2 is a current best practice to protect services against password cracking. This mechanism is, however, not impervious to dictionary attacks, as users frequently reuse their passwords on different services and may even use weak passwords.

What else can be done to improve the security of passwords for web services in general or in the event that a server's password file is leaked? Explain two mechanisms. **[4 marks]**

(d) What is the purpose of the Diffie–Hellman key exchange protocol? Describe the protocol. **[5 marks]**

3. **(a)** Suppose that the implementation of a simple messaging system uses DES in ECB mode. You are tasked with decrypting a 800 bytes long ciphertext generated by this messaging system. You don't have the decryption key, but you know that the plaintext is in English, and that the UTF-32 encoding is used in which every character (letter) is represented by four bytes.

How will you attempt to decrypt the ciphertext?

Hint: DES has a block length of 64 bits (8 bytes). **[5 marks]**

(b) Consider a hybrid encryption scheme with RSA and AES. The RSA public exponent is $e = 3$ and the modulus is 1024 bits, the AES key is 256 bits. Is RSA encryption padding essential in this case or would textbook RSA be sufficient? Justify your answer. **[5 marks]**

(c) Give an example of a replay attack on a protocol. Specify the protocol, then show the attack. What security property is violated? **[6 marks]**

(d) Over the last 30 years many cryptographic primitives and protocols have been designed and used. For each of the following primitives/protocols state what its purpose is and whether it is considered to be secure today:

RC4, SHA-1, AES, DES, ElGamal, Diffie-Hellman, TLSv1.3, SSLv2.0, CHACHA-20.

[9 marks]

4. (a) (i) A risk assessment of a company's system produced the following data:

Issue	Frequency (per year)	Damage (per incident)
User Data Confidentiality Breach	0.1	£1,000,000
Denial of Service Attacks	10	£25,000
Vandalized Website	20	£10,000

How should the risks be prioritized? **[3 marks]**

(ii) An evaluation of the countermeasures and funds required to mitigate the above threats produced the following data.

Issue	Mitigation costs (per year)
User Data Confidentiality Breach	£90,000
Denial of Service Attacks	£100,000
Vandalized Website	£10,000

The company has a fixed budget of £100,000 per year to spend on mitigating security vulnerabilities. How should this money be spent? Justify your answer. **[4 marks]**

(b) Explain what the purpose of onion routing is and how it works. **[4 marks]**

(c) Explain what a fork in the Bitcoin blockchain is and how it can be abused for double spending. **[6 marks]**

(d) Suppose your pseudorandom generator is broken. Its seed is a truly random 256-bit number. But every subsequent 256-bit number it generates is simply greater by 1 than the preceding one.

Suppose the pseudorandom generator is used to generate initialization vectors for the encryption of two different files f_1 and f_2, both of which are encrypted with AES-256-CTR and the same key k. How can an adversary learn information about the contents of f_1 and f_2? **[8 marks]**

END OF PAPER