This is an online, open book examination

THE UNIVERSITY OF MANCHESTER

Faculty of Science and Engineering

Department of Computer Science

COMP38411 Cryptography and System Security

Start time	9am 18/01/21
Duration	2 hours
Upload deadline	12pm

Instructions:

- Please answer **all** questions
- The examination is worth a total of **60** marks
- For full marks your answers should be concise as well as accurate
- Marks will be awarded for reasoning and method as well as being correct
- All students should do the exam independently

Your answers can be handwritten or typed. Please ensure your writing is legible and you clearly identify which part of the question your answer relates to. You must upload your answers as a single pdf document to the submission link at the end of the exam.

You are permitted one hour in addition to the exam duration in order to upload and submit your work. Please see the upload deadline in the table above.

Penalties for late submission

The time stamp of the upload will be used to determine if the work is late. You are strongly advised to upload your work as soon as the duration of the exam has ended.

If your work is submitted up to 60 minutes late of the upload deadline, your mark will be capped at the lowest compensatable mark . If you submit over 60 minutes late of the upload deadline, your mark will be 0.

Querying the examination

If you believe there is a mistake on the examination (typo, error with a question etc) then you can report this to SSO via email (compsci-sso@manchester.ac.uk) and it will be passed to the Unit Lead for checking. You will receive a direct response if no changes are made as a result of your query. If changes are required as a result of your query, the cohort will be advised via a Blackboard announcement **and** the amendment will be noted within the submission link instructions.

[Next page →]

1.

(a) Explain why a symmetric-key cipher, such as AES (Advanced Encryption Standard), and an asymmetric-key cipher, such as RSA, are often used together. (4 marks)

(b) Alice needs to send a very long message, *M*, to Bob. This message should be confidentiality protected. Alice and Bob have never met before and they do not have any prior trust. Propose the most efficient method by which Alice can send this confidential message to Bob over the Internet. (4 marks)

(c) Explain how to construct a stream cipher using an AES cipher, making clear how the encryption and decryption are carried out using the stream cipher. (4 marks)

(d) You are given a 20-byte long message. Give the mathematical equations for encrypting this message (4 marks) and for decrypting the ciphertext of the message (4 marks) using DES (Date Encryption Standard) in CBC (Cipher Block Chaining) mode.

2.

(a) Explain how a secure hash function can be used to authenticate a message. In your explanation, you should also make clear how verification is performed. (4 marks)

(b) The following is an authentication protocol designed for achieving mutual authentication between a client (e.g. Alice) and a server (Bob) during a logon session. It is assumed that any client can open multiple simultaneous sessions with Bob. Identify all possible means by which Eve may successfully log into Bob with Alice's identity. (6 marks)

Assumptions used in the protocol below:
Alice and Bob shares a secret key, K;
E is a symmetric-key cipher;
N_A and N_B are, respectively, the nonces contributed by Alice and Bob;
"X → Y: M" denotes X sends Y a message, M;
"x, y" denotes the concatenation of x and y.

Authentication protocol:
1. Alice → Bob: I am Alice, N_A
2. Bob → Alice: N_B, $E_K(N_A)$
3. Alice → Bob: $E_K(N_B)$

[Next page →]

(c) Design a method using the Diffie-Hellman algorithm so that three parties, Alice, Bob and Carole, could establish a shared symmetrical key to facilitate confidential group communication among the three parties. (4 marks)

Is there any security threat that should be addressed to ensure the security of the symmetrical key established? If so, explain the threat and propose a countermeasure to address the threat? (6 marks)

3.

Alice, a consumer, has been issued with a Chip&Pin payment card by her bank, hereafter referred to as the Issuer (i.e. the Issuer is the bank serving Alice). A card reader at the till of the Fashion store is owned by another bank, hereafter referred to as the Acquirer (i.e. the Acquirer is the bank serving the Fashion store). Both the Issuer and the Acquire are governed by a payment CA (Certification Authority), called Pay-CA. Pay-CA has got a pair of RSA keys, {PK_{CA}, SK_{CA}}, where PK_{CA} is Pay-CA's public key and SK_{CA} is Pay-CA's private key. The certificate certifying PK_{CA} has been uploaded onto the card reader.

The Issuer has also got a pair of RSA keys, {PK_{Iss}, SK_{Iss}}, where PK_{Iss} is the Issuer's public key, SK_{Iss} is the Issuer's private key, and PK_{Iss} has been certified by Pay-CA using SK_{CA}. To support an authorised use of the payment card, the Issuer has signed some verifiable data using SK_{Iss} and uploaded the signed data along with its public key certificate (certifying PK_{Iss}) onto Alice's payment card.

Now Alice is making a payment for her shopping in the Fashion store using her payment card via the card reader at the till in the store. During the payment process, the card reader fetches the signature signed by the Issuer and the Issuer's public key certificate from the payment card, and verifies the signature using the public key in the certificate. If the outcome of this verification is positive, which means that the payment card is authentic, then the card reader will process the payment. Otherwise, it will reject the card.

Answer the following questions.

(a) Highlight all the verifications the card reader should perform to verify the authenticity of the payment card. (4 marks)

(b) Identify any security weaknesses (or loopholes) in this payment method. (4 marks)

(c) Modify the payment method to overcome the weaknesses identified in (b). (6 marks)

(d) Based on your modified payment method given in (c), describe how the authenticity of the payment card is assured. In your description, you should make clear any data or messages that are sent between the two entities (i.e. the payment card and the card reader), as well as the operations that are performed by each of the entities. (6 marks)

END OF EXAMINATION