A36924

Calculators may be used in this examination provided they are not capable of being used to store alphabetical information other than hexadecimal numbers



UNIVERSITY OF BIRMINGHAM

School of Computer Science

Fourth Year Undergraduate/Postgraduate

06-34231

LM Network Security + Cryptography

Main Summer Examinations 2025

Time allowed: 2 hours

[Answer all questions]

Note

Answer ALL questions. The paper will be marked out of 100.

Question 1 Symmetric-Key Cryptography

(a) Recall that 3DES is a block cipher that encrypts a 64 bit block with a key of length $3 \times 56 = 168$ bits. 3DES consists of three calls to DES. Write short notes to compare 3DES with AES-128 in terms of

(i) *security*; **[7 marks]**

(ii) *performance*. **[7 marks]**

(b) Alice runs a club with 100 members and wants to organise a vote among them. Members will use an app to encrypt their vote with 3DES using a key that has been shared with the club members, and then they will send the output of the app by email to Alice. The vote text fits into a DES block. Alice programs the voting app to encrypt votes using ECB mode.

(i) Does this encryption mode provide *confidentiality of votes* from network intermediaries (such as the email service provider)? Briefly explain your answer. **[7 marks]**

(ii) Does this encryption mode provide *protection of vote integrity* from network intermediaries? Briefly explain your answer. **[7 marks]**

(c) Suppose two parties A and B share two symmetric keys K_1 and K_2. A wants to send a message M to B using *authenticated encryption*. A has access to the following primitives:

- Enc(x, y) which returns the encryption under key x of a message y, using CTR block mode;
- MAC(x, y) which computes a message authentication code, using key x, of a message y;
- Concat(x, y) which returns the concatenation of two messages x and y;
- Send(x) which sends the message x to B.

Using these primitives, write pseudocode for Alice to send the authenticated encryption of a message M. Both keys K_1 and K_2 are available to be used. **[7 marks]**

Question 2 Public-Key Cryptography

(a) Explain briefly

(i) Why the efficient algorithms to compute natural logarithm do not work for discrete log. **[3 marks]**

(ii) Why textbook RSA is not directly used for public-key encryption. **[3 marks]**

(b) In hybrid encryption, the message is encrypted using a symmetric key encryption scheme, and techniques involving public-key are used to communicate the symmetric key. Provide an example of a hybrid encryption scheme using Diffie-Hellman and AES. You need to write the encryption and the decryption algorithm. **[9 marks]**

(c) Bob decides to modify the ElGamal encryption scheme by changing the parameters and the Encryption algorithm as follows. Let the primes p, q and the element g same as in ElGamal encryption. $SK = x \xleftarrow{\$} \mathbb{Z}_q$, and $PK = g^x \mod p$

$\mathsf{Encrypt}(PK, m)$
$r \xleftarrow{\$} \mathbb{Z}_q$
$c_1 = g^r$
$c_2 = m^2 \cdot PK^r$
return (c_1, c_2)

As a cryptography auditor would you accept this modification? Justify your answer. **[9 marks]**

(d) Alice decides to batch-process Schnorr signature generation by modifying the sign algorithm to compute signatures of two messages at a time. Recall that $SK = x \in \mathbb{Z}_q$ and $PK = (g \in \mathbb{Z}_p^*, g^x, q, p)$ for primes p, q.

$\mathsf{ModifiedSign}(SK = x, M_1, M_2)$
$r_1 \xleftarrow{\$} \mathbb{Z}_q$
$s_1 = \mathcal{H}(M_1 || g^{r_1}) \quad t_1 = r_1 + x s_1 \mod q$
$r_2 = r_1 s_1 \mod q$
$s_2 = \mathcal{H}(M_2 || g^{r_2}) \quad t_2 = r_2 + x s_2 \mod q$
$\sigma_1 = (s_1, t_1) \quad \sigma_2 = (s_2, t_2)$
return (σ_1, σ_2)

As a cryptography auditor would you accept this modification? Justify your answer. **[9 marks]**

Question 3 Network security

A small start-up company is discussing the choice of their main platform for online discussions. The company doesn't have its own offices and often the executives operate from cafés or other public places using unsecured wifi. The candidates they are considering are: *Gmail* (Google email), and the *Signal app*. The company's requirements are:

- Confidentiality: no-one outside the company should be able to access company discussions. In particular, service providers (such as Google, Signal, and the providers of public wifi networks) should not be able to access company discussions.
- Integrity: no-one should be able to delete messages, alter messages, or create fake messages, or to change the order of messages in conversations. Again, in particular, service providers should not be able to do this.

(a) Briefly explain whether *Gmail* provides a solution satisfying the company's requirements for *confidentiality*. **[8 marks]**

(b) Briefly explain whether *Gmail* provides a solution satisfying the company's requirements for *integrity*. **[8 marks]**

(c) Briefly explain whether *Signal* provides a solution satisfying the company's requirements for *confidentiality*. **[8 marks]**

(d) Briefly explain whether *Signal* provides a solution satisfying the company's requirements for *integrity*. **[8 marks]**

In your explanations, please be sure to explain if there are any encryption keys involved, where they are located, and (if needed) how they are certified for *integrity*.

This page intentionally left blank.

Do not complete the attendance slip, fill in the front of the answer book or turn over the question paper until you are told to do so

Important Reminders

- Coats/outwear should be placed in the designated area.
- Unauthorised materials (e.g. notes or Tippex) must be placed in the designated area.
- Check that you do not have any unauthorised materials with you (e.g. in your pockets, pencil case).
- Mobile phones and smart watches **must** be switched off and placed in the designated area or under your desk. They must not be left on your person or in your pockets.
- You are not permitted to use a mobile phone as a clock. If you have difficulty seeing a clock, please alert an Invigilator.
- You are not permitted to have writing on your hand, arm or other body part.
- Check that you do not have writing on your hand, arm or other body part – if you do, you must inform an Invigilator immediately
- Alert an Invigilator immediately if you find any unauthorised item upon you during the examination.

Any students found with non-permitted items upon their person during the examination, or who fail to comply with Examination rules may be subject to Student Conduct procedures.