UNIVERSITY OF BRISTOL

Summer Resit Period 2025

Faculty of Engineering

Examination for the Degrees
of
Bachelor of Science
Master of Engineering
Master of Science

COMS30085— Mid-Term Assessment
Cryptology

TIME ALLOWED:
50 Minutes

This paper contains 3 questions over 5 pages.
Answer all the questions.
The maximum for this paper is 50 marks.

Other Instructions

1. **This is an open book exam.**
2. **All computing devices are permitted.**

TURN OVER ONLY WHEN TOLD TO START WRITING

Preamble

This mid-term exam is composed of 3 questions, *all* of which you must answer. Questions are grouped thematically. Within each question, question parts are roughly ordered by increasing difficulty (as *we* perceive it, and as much as possible while maintaining cohesion). Expected difficulty is based on the complexity of the material, the depth of understanding required, *and* the level of guidance given. Because we assess different skills with each question, your own perception of relative difficulty may be different. Questions marked with a $\star$ are those we intend for the 80-100 range of marks.

Use of calculators and computers. You are free to use a computer or calculator throughout, but *must* show your working where specified. For more advanced questions, we expect you to use Sage or Python, both of which should be available on your computers. As a last resort, you can use Sage online via CoCalc.[1] Where we ask you to "Show your working", and where appropriate, a short annotated code snippet demonstrating your understanding of the techniques you are using will be accepted.

Open Book and Referencing. This is an open book exam conducted with access to the internet. If you reference external material (material that we did not provide during the course of the unit) or use external tools (including AI-enabled tools) to produce your answers, you *must* include clear references, in line with the University's academic integrity policy.[2] If you use AI-enabled tools, keep in mind that you are taking responsibility for the content of the answers you write down in your answer booklet, including when it comes to academic misconduct.

Marking Scale. Partial marks will be given for answers that demonstrate general understanding but get details wrong (or forget them). In general (and where possible without fractional marks), getting 50% of the way to a full answer should net you roughly 70% of the marks. Effort beyond that will offer diminishing returns, so plan your work accordingly, and give yourself time and space to iterate on more complex questions.

[1] https://cocalc.com/

[2] https://www.bristol.ac.uk/academic-quality/academic-integrity/

Q1 — Symmetric Cryptography [15 marks]

This question is about symmetric cryptography.

$\underline{\mathsf{Keygen}()}$
$\quad \mathsf{k} \xleftarrow{\$} \mathcal{K}$
$\quad \textbf{return } \mathsf{k}$

$\underline{\mathsf{Enc}^{\mathsf{n}}_{\mathsf{k}}(\mathsf{m}_0 \| \ldots \| \mathsf{m}_b)}$
$\quad \mathsf{x} \leftarrow \mathsf{n}$
$\quad \textbf{for } \mathsf{i} \in [0, b-1]$
$\quad\quad \mathsf{c}_\mathsf{i} \leftarrow \mathsf{m}_\mathsf{i} \oplus \mathsf{E}_\mathsf{k}(\mathsf{x})$
$\quad\quad \mathsf{x} \leftarrow \mathsf{m}_\mathsf{i} \oplus \mathsf{x}$
$\quad \textbf{return } \mathsf{c}_0 \| \ldots \| \mathsf{c}_b$

Figure 1: A Mode of Operation, using a blockcipher E with key space $\mathcal{K}$.

Consider the mode of operation shown in Figure 1.

[3 marks] **1.a)** Define decryption for this mode of operation.

[2 marks] **1.b)** Does this scheme support parallel decryption?

[5 marks] **1.c)** Show that this mode of operation is not (N)IND-CPA-secure as an nonce-based encryption scheme even when E is secure as a blockcipher.

[5 marks] **1.d)** $\star$ This scheme is not (IV)IND-CPA-secure as an IV-based encryption scheme. Show a distinghuisher whose advantage is close to 1, and that makes 1 chosen-plaintext query and almost no computation. The query will likely be at least 2 blocks long.

Q2 — Definitions [10 marks]

This question is about security definitions, and how we formally relate them.

$\underline{\mathsf{Exp}^{\mathsf{ind\text{-}cpa\text{-}real}}_{\mathsf{E}}(\mathbb{A})}$
$(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{E.Keygen}()$
$\mathsf{m} \xleftarrow{\$} \mathbb{A}(\mathsf{pk})$
$\mathsf{c} \xleftarrow{\$} \mathsf{E.Enc}_{\mathsf{pk}}(\mathsf{m})$
$\mathsf{b} \xleftarrow{\$} \mathbb{A}(\mathsf{pk}, \mathsf{c})$

$\underline{\mathsf{Exp}^{\mathsf{ind\text{-}cpa\text{-}ideal}}_{\mathsf{E}}(\mathbb{A})}$
$(\mathsf{pk}, \mathsf{sk}) \xleftarrow{\$} \mathsf{E.Keygen}()$
$\mathsf{m} \xleftarrow{\$} \mathbb{A}(\mathsf{pk})$
$\mathsf{c} \xleftarrow{\$} \mathcal{C}$
$\mathsf{b} \xleftarrow{\$} \mathbb{A}(\mathsf{pk}, \mathsf{c})$

$$\mathsf{Adv}^{\mathsf{ind\text{-}cpa}}_{\mathsf{E}}(\mathbb{A}) = \left|\mathsf{Pr}\left[\mathsf{Exp}^{\mathsf{ind\text{-}cpa\text{-}real}}_{\mathsf{E}}(\mathbb{A}) : b\right] - \mathsf{Pr}\left[\mathsf{Exp}^{\mathsf{ind\text{-}cpa\text{-}ideal}}_{\mathsf{E}}(\mathbb{A}) : b\right]\right|$$

Figure 2: A candidate security notion for public-key encryption.

[3 marks] **2.a)** Consider the notion of IND-CPA security for *public key* encryption shown in Figure 2. Is this definition reasonable? Briefly justify your answer from basic principles of modern cryptography and the intended security notion of indistinguishability (from random) under chosen plaintext attacks.

[7 marks] **2.b)** Argue that RSA encryption, as seen in lectures, does not have IND-CPA security as defined in Figure 2.

Q3 — Key Exchange, Public Key Encryption [25 marks]

[4 marks] **3.a)** Using double-and-add, show that $34 \times 49 = 1666$

3.b) In the Diffie-Hellman key exchange scheme, Alice wants to agree a shared secret with Bob. However that pesky Eve is meddling again. The public parameters of the system are $p = 107$ and $g = 5$

[3 marks] i. Alice chooses her private parameter $a = 20$ and Bob chooses his private parameter $b = 17$. What does Alice send to Bob, what does Bob send to Alice and what is their shared secret?

[3 marks] ii. Meddlesome Eve wants to cause some mischief: she stops Alice's message reaching Bob and she stops Bob's message reaching Alice. Instead, she'll send $g^e = 15$ to both Alice and Bob, masquerading as Bob's and Alice's public keys respectively.
What shared secret does Alice think she's agreed with Bob? What shared secret does Bob think he's agreed with Alice?

[2 marks] iii. Comment on the effect of Eve's interference.

3.c) Recall how to encrypt in the Elgamal cryptosystem:

Public Key Setup: Choose a prime p, and a generator g of $\mathbb{Z}/p\mathbb{Z}^*$. Choose a random secret $r \in \{1, \ldots, p-1\}$ and computes $pk = g^r \pmod p$. The public key is (p, g, pk).

Encryption: Pick a random secret $h \in \{1, \ldots, p-1\}$ and compute the shared secret $s = pk^h \pmod p$. Encrypt the message as $enc_m = m \cdot s$. Send the ciphertext $(g^h \pmod p, enc_m)$.

[3 marks] i. Take $p = 83$, $g = 5$, $r = 4$, $h = 11$, and $m = 10$. Calculate the ciphertext.

[2 marks] ii. How would you check that g is a generator of $\mathbb{Z}/p\mathbb{Z}^*$? You do not have to do it.

[3 marks] iii. Is 32 a generator of $\mathbb{Z}/41\mathbb{Z}^*$? Justify your answer.

[5 marks] **3.d)** i. $\star$ Alice wants to send Bob a message using RSA. Her public key is: $(N_A = 519504677238793, e = 7)$. She encrypts the message $m = 49$ to the ciphertext $c = 678223072849$. Would an adversary have to factor N_A to recover m from c? Explain your answer.

THIS IS THE END OF THE EXAM