UNIVERSITY OF BRISTOL

October 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:
1 Hour

This paper contains 4 questions over 6 pages.
Answer all the questions.
The maximum for this paper is 50 marks.

<u>Other Instructions</u>
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 4 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). Indicative 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. We encourage you to read the whole set of questions before getting started on those we intend as easy, especially since there may be easy marks to glean by simply restating hard questions in formal terms relevant to the unit.

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 also 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/