Midterm info

From Canvas's announcement:

Mid Term

- Date: 9 October
- Venue: MPSH 1A&1B
- Time: Start at 14:15pm. End 15:15pm. Students expected able to leave before 15:30pm. Hall opens 14:05pm.

- Coverage:
  - Lecture: Topic 0, 1, 2, 3.
  - Tutorial: 1,2,3,4,5
- Format:
  - Closed book. One A4 double-sided cheat sheet.
  - Calculator, including Scientific and Graphing Calculator, are allowed. All calculation, if any, can be easily done by hand.
  - MCQ, fill-in-the-blank, short questions.

Additional info:

1. Keywords that might appear:
   PKCS#1, authenticated encryption, padding oracle, textbook RSA, digest, mac, signature, birthday attack, encrypt-then-mac.

2. The term "encrypt-then-mac" would appear later in lecture. Given an message $\boldsymbol{m}$ and key $\boldsymbol{k_1}$, $\boldsymbol{k_2}$ for encryption and mac respectively, the process of first encrypt $\boldsymbol{m}$ using $\boldsymbol{k_1}$, and then concatenate with the mac of the ciphertext using $\boldsymbol{k_2}$ is known as *encrypt-then-mac*. It is a secure way to achieve authenticated encryption, i.e. achieve both confidentiality and authenticity.
   Let c= Enc($\boldsymbol{k_1}$, m). The final ciphertext is c || mac ($\boldsymbol{k_2}$, c)

3. The term "PKCS#1" would appear. Its actual construction is not included in the lecture note and not required for this test.

Cover page and answer sheet

CS2107 —Introduction to Information Security
School of Computing
National University of Singapore

Midterm Test

2025/2026 Semester 1

9 October 2025 **Time allowed:** 1 hour

Instructions (please read carefully):

1. This is a **CLOSED** book assessment, but you are allowed to bring **ONE** double-sided A4 sheet of notes for this assessment.
2. The assessment paper contains **SEVENTEEN (17) questions** and comprises TEN (10) pages including this cover page.
3. The time allowed is **1 hour**.
4. Use of calculators is allowed in the test.
5. You are allowed to use pencils, ball-pens or fountain pens. No red color.
6. **Marks may be deducted** for unrecognizable handwriting. All corrections should be cleanly erased or covered with correction fluid or tape.

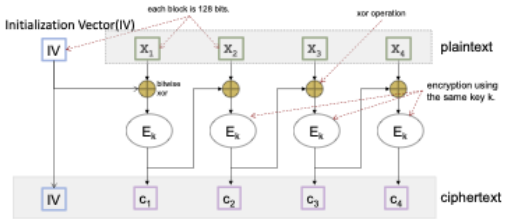
Instructions for ANSWER SHEET:

1. Write down your **student number** in the answer sheet and shade the corresponding circles with dark ink or pencil.
2. DO NOT WRITE YOUR NAME!
3. The answer sheet comprises 2 pages.
4. You must submit only the **ANSWER SHEET** and no other documents. The question set may be used as scratch paper.
5. All answers must be written within the corresponding box provided. **Anything written outside the answer box will not be accepted.**

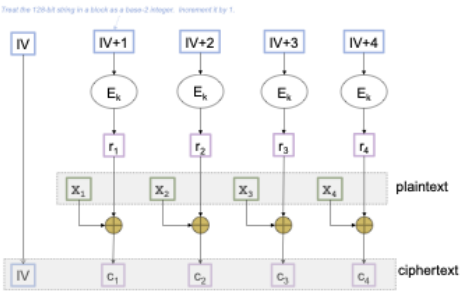
GOOD LUCK!

References

1. Guideline on key strength in this mid-term:
   (a) Exhaustive search over 100-bit keys is feasible. That is, 2^{100} number of cryptographic operations is feasible.
   (b) To secure against online dictionary attack, password entropy of 49 bits is sufficient.
   (c) To secure against offline dictionary attack, password entropy of 128 bits is sufficient.
2. ASCII representation of "0", "1", and "2" in hexadecimal is `30`, `31`, and `32` respectively.
3. The notation || refers to string concatenation. E.g. "AB" || "C" = "ABC".
4. Description of CBC mode encryption from lecture note.



5. Description of CTR mode encryption from lecture note.



Multiple Choice Questions [32 marks]

(Each question is worth 2 marks and has only one correct answer).

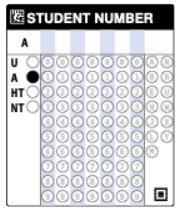
Short Answer Section [18 marks]

Each "YES"/"NO" question is worth 1 mark, making a total of 6 marks. The total for the explanation is 12 marks.

Submit only the “Answer sheet”. Below are example of answer sheet. The actual sheet is different.

CS2107 Introduction to Information Security

Midterm Test — Answer Sheet



FOR EXAMINER'S USE	
Question	Marks
Q1-Q16	/ 32
Q17 (Y or N)	/ 6
Q17 (short Q)	/ 12
Total	/ 50

1. ○ A ○ B ○ C ○ D
2. ○ A ○ B ○ C ○ D
3. ○ A ○ B ○ C ○ D
4. ○ A ○ B ○ C ○ D
5. ○ A ○ B ○ C ○ D
6. ○ A ○ B ○ C ○ D
7. ○ A ○ B ○ C ○ D
8. ○ A ○ B ○ C ○ D
9. ○ A ○ B ○ C ○ D
10. ○ A ○ B ○ C ○ D
11. ○ A ○ B ○ C ○ D
12. ○ A ○ B ○ C ○ D
13. ○ A ○ B ○ C ○ D
14. ○ A ○ B ○ C ○ D
15. ○ A ○ B ○ C ○ D
16. ○ A ○ B ○ C ○ D

17. (a) ○ YES ○ NO

(b) ○ YES ○ NO

(c) ○ YES ○ NO

(d) ○ YES ○ NO

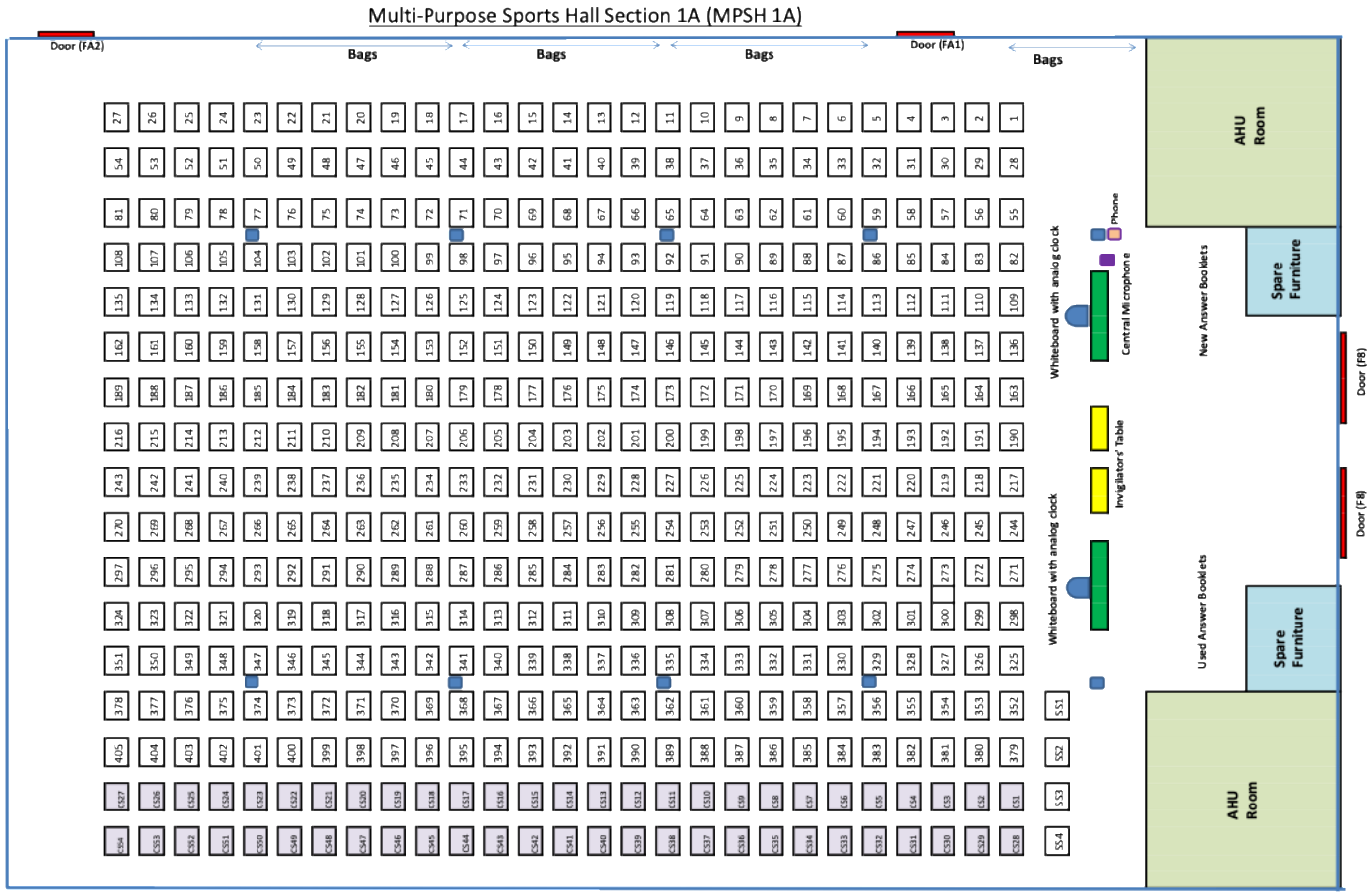
(e) ○ YES ○ NO

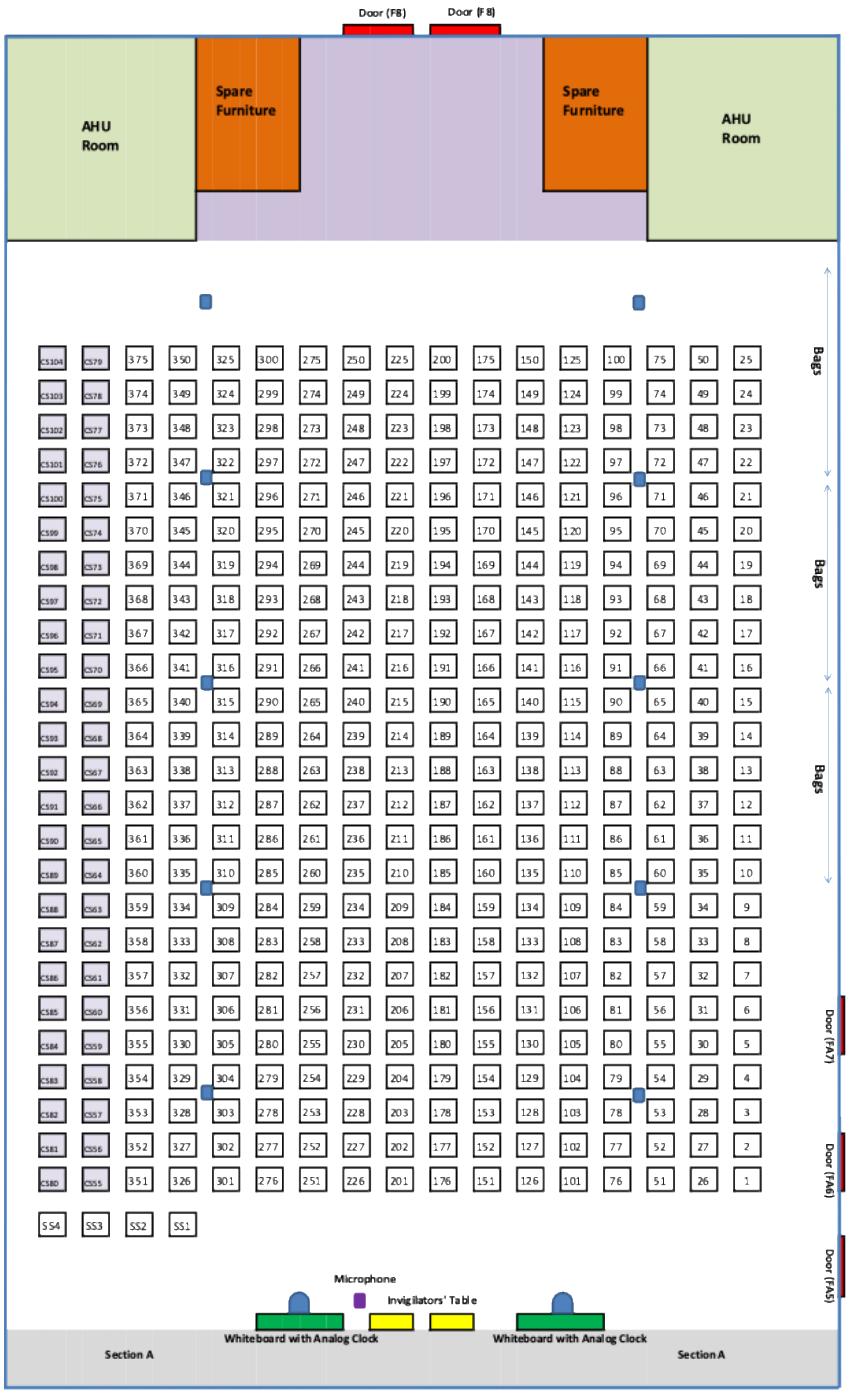
(f) ○ YES ○ NO

— END OF ANSWER SHEET —

Seating.

- Each student has an assigned seat. The list is uploaded to Canvas. Contact Prof Nitya if you name is not in the list.





Multi-Purpose Sports Hall Section 1B (MPSH 1B)