Version A

ECE 422 – Midterm exam
Winter 2024
Monday, February 26, 2024
Duration: 45 minutes

An Ran Chen
anran6@ualberta.ca

University of Alberta
Department of Electrical and Computer Engineering

Instructions

– Answer all questions on these sheets in the space provided.
– No books, notes or extra paper.
– No cell phones, laptops or any electronic devices except approved non-programmable calculators.
– This exam is 9 pages long, including the cover page. It has 22 questions labeled from question 1 to question 22. Check that your copy is complete.
– This exam is graded on 25 points.
– This exam counts for 25% of your final grade.

Consistent with the university regulations concerning cheating and plagiarism I will not cheat during this examination:

Student ID:_____

First Name / Last Name:_____

Signature:_____

Version A

I. True/False questions [3 points]

Question 1 [0.5 pts]
SRE is an implementation of the practices that DevOps describes.

- [x] True
- [ ] False

Question 2 [0.5 pts]
SLI is an agreement within an SLA about a specific metric like uptime or response time.

- [ ] True
- [x] False, SLI is the actual performance metric.

Question 3 [0.5 pts]
An example of crash failure describes the situation where the server has no response to incoming requests.

- [ ] True
- [x] False, crash failure implies when the server has valid responses until it crashes.

Question 4 [0.5 pts]
Fail-noisy failures describe halting failures that are eventually and reliably detected.

- [x] True
- [ ] False

Question 5 [0.5 pts]
N-version programming runs individual acceptance tests for each version of the system, and returns the majority agreement as output.

- [ ] True
- [x] False, N-version programming executes N versions in parallel, and returns the majority agreement as output.

Question 6 [0.5 pts]
In an HMAC-based one-time password implementation, the server synchronizes the counter variable with the application before each passcode generation.

- [ ] True
- [x] False, the counter variable synchronization happens after the passcode has been verified.

II. Multiple Choice Questions [4 points + 0.5 bonus point]
Please encircle the right choice for the following questions.

Question 7 [0.5 point]
What does the CMD instruction do in Dockerfile?

a. Execute build commands
b. Specify default commands
c. Create a new stage from a base image
d. Change working directory

Question 8 [0.5 point]
Which process prioritizes on delivering changes through rigorous automated testing in the staging phase?

a. Continuous deployment
b. Continuous integration
c. Continuous delivery
d. Continuous testing

Question 9 [0.5 point]
The course instructor creates hashes of student project files in order to monitor whether information has been tampered with the ones submitted through GitHub. The above scenario verifies what property of the project?

a. Availability
b. Confidentiality
c. Integrity
d. Irreversibility
e. Redundancy

Question 10 [0.5 point]
On the trade-offs between reliability and security, a redundant solution makes the system fail _____. It provides alternative solutions in case of failure. However, it increases the attack surface.

a. safely
b. redundantly
c. securely
d. reliably

Question 11 [0.5 point]
Which one of the following helps upgrade the security of a current authenticator apps authentication system to a multi-factor authentication system? (select all possible choices)

a. Access card - possession
b. PIN code - knowledge
c. Fingerprint - biological
d. IP address - location
e. All of the above

Question 12 [0.5 point]
Which of the following statements is the most likely to be suspicious based on Spectrum-based Fault Localization?

	T_1	T_2	T_3
S_1	✓		
S_2		✓	✓
S_3	✓		
S_4	✓	✓	✓
Result	P	F	F

$$Ochiai(element) = \frac{e_f}{\sqrt{(e_f + n_f) \cdot (e_f + e_p)}}$$

a. S_1
b. S_2
c. S_3
d. S_4

Question 13 [0.5 point]
Given that 0001011 is a codeword in (7, 4) Hamming code, which of the following cannot be the valid codeword in the codespace? (Hint: a (7, 4) Hamming code can correct and detect any single-bit error.)

a. 0011101
b. 0101100
c. 0011010, a code distance = 2
d. 1110100

Question 14 [0.5 point]
Consider the following statements, which ones are true?

1. 100% statement coverage guarantees 100% branch coverage.
2. 100% branch coverage guarantees 100% statement coverage.
3. 100% path coverage guarantees 100% statement coverage.
4. 100% path coverage guarantees 100% branch coverage.
5. 100% statement coverage guarantees 100% path coverage.

a. Statement 2
b. Statements 1 and 5
c. Statements 2 and 3
d. Statements 2, 3, and 4, 100% branch coverage implies 100% statement coverage. 100% path coverage implies 100% branch and statement coverage. Therefore, statements 2, 3, and 4 are true.

Question 15: Bonus question [0.5 point]
What is the probability that at least two people have the same birthday in our classroom (Hint: we are a class of 78 people)?

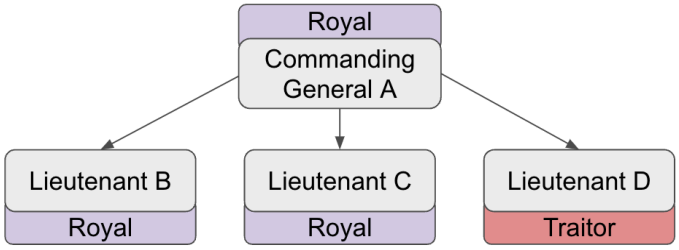
a. 12%
b. 50%
c. 97%
d. 99%

III. Short Answer Questions [8 points]

Question 16 [2 points]
a) Given a (255, 247) Hamming code, how many parity bits does it have?
Answer: 8 parity bits

b) What is its information rate? (Hint: information rate = k/n)
Answer: 97% information rate

Question 17 [3 points]
Given the following Byzantine general problem where the Commanding General A sends an “attack” message to others.



a) Will Lieutenant B and C attack? Show their decision making process (e.g., V(D) = (R, R, A) where A denotes attack, R denotes retreat).
Answer: Both general B and C will attack at the same time.
V(B) = (A, A, R)
V(C) = (A, A, R)

b) Is consistency satisfied? If yes, why? If not, why not?
Answer: Yes, B and C executed the same order.

c) Is validity satisfied? If yes, why? If not, why not?
Answer: Yes, B and C obeyed the order from A.

Question 18 [3 points]
a) Name the most secure access control model.
Answer: Mandatory access control (MAC)

b) Who controls the resources?
Answer: Administrator

c) Give a brief description of how the resources are protected (i.e., how users gain access).
Answer: Users can only access the resource when their security labels entitles the access

III. Computational Questions [10 points]

Question 19 [2 points]
Alice wants to send a message (m = 5) to Bob through the RSA algorithm. Assume that the two prime numbers used to generate the keys are p = 5, q = 11, and Alice must choose a value e < 6. What is the ciphertext? (show your calculations and assumptions)

Hint:

- $m^e \bmod(n) = c$
- $c^d \bmod(n) = m$

Answer: The ciphertext is 15.
With RSA, we perform the following calculations:
n = pq = 55 (0.5 pts)
φ(n) = (p - 1)(q - 1) = 4 x 10 = 40 (0.5 pts)
Condition: 1 < e < φ(n), and given that e < 6. Therefore, 1 < e < 6
Condition: e and φ(n) must be coprime. Therefore, e cannot be a divisor of 40 including 2, 4, 5
Since e must be less than 6, it must be 3.
$c = m^e \bmod (n)$
$= 5^3 \bmod (55)$
= 15 (1 pt)

Question 20 [3 points]
In Question 19, Alice used the RSA algorithm to send the message (m = 5) to Bob so that others could not read the message. Suppose that you have been listening to their communication channel:

a) Do you know Alice's public key? If yes, what is it? (1~2 sentences) (1 pt)
Answer: No, the public and private key needed for encryption belong to Bob. Nothing is known about Alice's public key.

b) Do you know Bob's public key? If yes, what is it? (1~2 sentences) (1 pt)
Answer: Yes, Bob's public key is {3, 55}.

c) If Bob uses a digital signature, then what is its purpose? (i.e., what does the digital signature do?) (1~2 sentences) (1 pt)
Answer: The digital signature certifies that the public key belongs to Bob.

Question 21 [2 points]
Suppose g(x) = 1101 for a (7, 4) cyclic code. Bob receives a codeword 0010111 from Alice. Is there an error? If yes, justify why. If not, what is the original data? (show your steps)
Answer: No error, because remainder is null. The original data is 0011 (or 0011000).
$c(x) = x^2 + x^4 + x^5 + x^6$ (0.5 pts)
$g(x) = 1 + x + x^3$ (0.5 pts)
$d(x) = c(x)/g(x) = x^2 + x^3$ (1 pt)

Question 22 [3 points]
Calculate the final code after encoding the code 11110100100 into 16-bit even parity extended Hamming code. (show your steps, e.g., P_1: {0000001}, odd parity, P_1 = 1) (Hint: 1 111 010 0100)
Answer: 0001 0111 0010 0100
P_1: {1110010}, even parity, P_1 = 0 (0.6 pts)
P_2: {1111000}, even parity, P_2 = 0 (0.6 pts)
P_3: {1110100}, even parity, P_3 = 0 (0.6 pts)
P_4: {0100100}, even parity, P_4 = 0 (0.6 pts)
P_5: {001011100100100}, even parity, P_5 = 0 (0.6 pts)