Lecture 18
Midterm Review

ECE 422: Reliable and Secure Systems Design

UNIVERSITY OF ALBERTA

Instructor: An Ran Chen
Term: 2024 Winter

How was the midterm?

A quick survey: [Click here for the survey link]

- How hard was the midterm?
- Did you know what to study for your midterm?
- Did you have enough support (e.g., materials, sample questions) to prepare for the midterm?

Question on (7, 4) Hamming code

Multiple Choice Question: 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
d. 1110100

Code distance in error correction

To correct *d* bit errors, the code distance for the codewords must be larger or equal to *2d+1*.

Example

Code: {000, 101}

$C_d = 2$

Transmitting codeword: 000

A single-bit error happens, 000 becomes 001

We cannot tell how to correct 001 (000 or 101).

Analogy

Dictionary: {accept, except}

Distance = 2

Typed word: accept

A typo happens, accept becomes eccept

We cannot tell which word is mistyped.

Question on (7, 4) Hamming code

Multiple Choice Question: 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

d. 1110100

To correct *d* bit errors, the code distance for the codewords must be larger or equal to *2d+1*.

0	0	0	1	0	1	1	
0	0	1	1	1	0	1	→ distance = 3
0	1	0	1	1	0	0	→ distance = 5
0	0	1	1	0	1	0	→ distance = 2
1	1	1	0	1	0	0	→ distance = 7

Question on Spectrum-based Fault Localization

Multiple Choice Question: Which of the following statements is the most likely to be suspicious based on Spectrum-based Fault Localization?

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

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

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

Lecture 6: Spectrum-based fault localization

Failed test

Source file **A**

Run tests

	T_1	T_2	T_3
S_1	✓		
S_2		✓	
S_3		✓	✓
S_4	✓	✓	

Execution profiles

SBFL

Statement	Suspiciousness score
S_1	0.00
S_2	0.71
S_3	1.00
S_4	0.50

Hint: program elements that are covered by more failing tests but less passing tests are more suspicious.

Question on Spectrum-based Fault Localization

Multiple Choice Question: Which of the following statements is the most likely to be suspicious based on Spectrum-based Fault Localization?

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

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

S_2: 2 failing tests
S_4: 2 failing tests, 1 passing test

S_2 is the most suspicious statement

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

Question on RSA algorithm

Alice wants to send a message ($m = 5$) to Bob. Assume that the two prime numbers used to generate the keys are $p = 5$, $q = 11$, and Alice must choose a value $e < 6$.

Question: What is the ciphertext? (show your calculations and assumptions)

[2 points]

Encryption key (e, n)

- $m^e \ mod(n) = c$

Question on RSA algorithm

Alice wants to send a message ($m = 5$) to Bob. Assume that the two prime numbers used to generate the keys are $p = 5$, $q = 11$, and Alice must choose a value $e < 6$.

Question: What is the ciphertext? (show your calculations and assumptions)

Thought process: We have the values m, p, q, asked to calculate c

- We need to calculate the public key (e, n) to find c
  - Step 1: calculate n
  - Step 2: calculate $\varphi(n)$
  - Step 3: find e that satisfies the conditions
  - Step 4: calculate c with (e, n)

Lecture 17: RSA algorithm

Part I: Bob's public and private key setup

- Chooses two prime numbers, p and q
- Calculate the product $n = pq$
- Solve $\varphi(n) = (p-1)(q-1)$
- Choose numbers e and d so that ed has a remainder of 1 when divided by $\varphi(n)$
  - $1 < e < \varphi(n)$, *where e must be an integer*
  - *e and* $\varphi(n)$ *must be coprime*
- Publish the public key (e, n)

Example

- $p = 11$, $q = 3$
- $n = pq = 33$
- $\varphi(n) = 10 \times 2 = 20$
- Pick e and d so that ed = 20+1

  e.g.,: $e = 3$, $d = 7$
  - 1 < 3 < 20
  - 3 and 20 are coprime
- Publish $(e, n) = (3,$

Question on RSA algorithm

Solution: We need to calculate the public key (e, n) to find c

Step 1: calculate n

- If p = 5, q = 11, then n = pq = 55 [0.5 pts]

Step 2: calculate φ(n)

- φ(n) = (p-1)(q-1) = 4 x 10 = 40 [0.5 pts]

Question on RSA algorithm

Solution (cont.):

Step 3: find e that satisfies the conditions

- Condition: $1 < e < \varphi(n)$, and given that $e < 6$
    - $1 < e < 6$
- Condition: e and $\varphi(n)$ must be coprime
    - e and 40 must be coprime
    - e cannot be a divisor of 40 including 2, 4, 5
- Since e must be less than 6, it must be 3
- Public key: (3, 55)

Question on RSA algorithm

Solution (cont.):

Step 4: calculate c with (e, n)

Version A: If e = 3, m = 5

- $m^e \ mod(n) = c$
- 5^3 mod (55) = 15 [1 pt]

Version B: If e = 3, m = 7

- $m^e \ mod(n) = c$
- 7^3 mod (55) = 13 [1 pt]

Question on RSA algorithm

In previous question, 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:

Question: Do you know Alice’s public key? If yes, what is it? (1~2 sentences)

[1 point]

Question on RSA algorithm

In previous question, 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:

Question: Do you know Alice's public key? If yes, what is it? (1~2 sentences)

Thought process: Alice wants to send a message to Bob

- Alice should use Bob's public key to encrypt the message
  - Analogy: only Bob can open the envelope with his private key

Lecture 17: Asymmetric encryption

Asymmetric encryption uses a public key to encrypt and a private key to decrypt.

- Public key: anyone can see and use this key
- Private key: kept private
- Private and public keys come in pairs
- Data encrypted with the public key can only be decrypted with the private key

Suppose Alice needs to send a message to Bob

- Alice will use Bob’s public key to encrypt the message
- Bob will use his own private key to decrypt the message

Question on RSA algorithm

In previous question, 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:

Question: Do you know Alice's public key? If yes, what is it? (1~2 sentences)

Thought process: Alice wants to send a message to Bob

- Alice should use Bob's public key to encrypt the message
  - Analogy: only Bob can open the envelope with his private key
- Do we need Alice's public key? No

Solution: No, the public and private key needed for encryption belong to Bob. Nothing is known about Alice's public key.

Question on RSA algorithm

In previous question, 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:

Question: Do you know Bob's public key? If yes, what is it? (1~2 sentences)

[1 point]

Question on RSA algorithm

In previous question, 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:

Question: Do you know Bob's public key? If yes, what is it? (1~2 sentences)

Solution: Yes, Bob's public key: $(e, n) = (3, 55)$

Question on RSA algorithm

In previous question, 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:

Question: If Bob uses a digital signature, then what is its purpose? (i.e., what does the digital signature do?)

[1 point]

Question on RSA algorithm

In previous question, 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:

Question: If Bob uses a digital signature, then what is its purpose? (i.e., what does the digital signature do?)

Solution: The digital signature certifies that the public key belongs to Bob.

Digital signature

Digital signatures verify the authenticity

- Detect the identity of the sender/signer

Digital signatures check the integrity

- Verify that the message was not changed

Digital signatures ensure non-repudiation

- Verify that the signature is not fake

Question on cyclic codes

Suppose g(x) = 1101 for a (7, 4) cyclic code. Bob receives a codeword 0010111 from Alice.

Question: Is there an error? If yes, justify why. If not, what is the original data? (show your steps)

[2 points]

Question on cyclic codes

Suppose g(x) = 1101 for a (7, 4) cyclic code. Bob receives a codeword 0010111 from Alice.

Question: Is there an error? If yes, justify why. If not, what is the original data? (show your steps)

Thought process: We have the values g(x) and c(x), asked whether there is a remainder in c(x)/g(x). If yes, then there is a error.

- Solve d(x) = c(x)/g(x)
    - Step 1: convert c(x) and g(x) into polynomials
    - Step 2: calculate polynomial division c(x)/g(x), check for remainder

Question on cyclic codes

Suppose g(x) = 1101 for a (7, 4) cyclic code. Bob receives a codeword 0010111 from Alice.

Question: Is there an error? If yes, justify why. If not, what is the original data? (show your steps)

Solution: Solve d(x) = c(x)/g(x)

Step 1: convert c(x) and g(x) into polynomials

- $c(x) = x^2 + x^4 + x^5 + x^6$ (0.5 pts)
- $g(x) = 1 + x + x^3$ (0.5 pts)

Lecture 9: Step 1: data polynomial

Data = {1001}

The data can be represented as a polynomial:

$$a(x) = a_0.x^0 + a_1.x^1 + \ldots + a_{n-1}.x^{n-1}$$

The data can also be visualized as:

$$\underline{1}\ \underline{0}\ \underline{0}\ \underline{1}$$

$$\boxed{1 \cdot x^0} \quad \boxed{0 \cdot x^1} \quad \boxed{0 \cdot x^2} \quad \boxed{1 \cdot x^3}$$

So we represent 1001 as:

$$d(x) = 1 \cdot x^0 + 0 \cdot x^1 + 0 \cdot x^2 + 1 \cdot x^3 = 1 + x^3$$

Lecture 9 Slide 19
Lecture 10 Slide 9

Question on cyclic codes

Solution (cont.):

Step 2: calculate polynomial division c(x)/g(x), check for remainder

- $(x^2 + x^4 + x^5 + x^6)/(1 + x + x^3) = x^2 + x^3$, no remainder

$$
\begin{array}{r|l}
x^6 + x^5 + x^4 + x^2 & x^3 + x + 1 \\
\cline{2-2}
x^6 + x^4 + x^3 & x^3 + x^2 \\
\hline
x^5 + x^3 + x^2 & \\
x^5 + x^3 + x^2 & \\
\hline
0 &
\end{array}
$$

No remainder
No error

Lecture 10: Polynomial division (1)

$$
\begin{array}{l|l}
x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 & x^3 + x + 1 \\
\hline
x^6 + x^4 + x^3 & x^3 + x^2 + 1 \\
\hline
x^5 + x^2 + x + 1 & \\
x^5 + x^3 + x^2 & \\
\hline
x^3 + x + 1 & \\
x^3 + x + 1 & \\
\hline
0 &
\end{array}
$$

No error

Question on cyclic codes

Suppose $g(x) = 1101$ for a (7, 4) cyclic code. Bob receives a codeword 0010111 from Alice.

Question: Is there an error? If yes, justify why. If not, what is the original data? (show your steps)

Solution: The original data is 0011 (or 0011000) (1 pt)

- Partial mark: $x^3 + x^2$ (0.5 pts)

Question on extended Hamming code

Question: Calculate the final code after encoding the code 11110100100 into 16-bit even parity extended Hamming code. (show your steps, e.g., P1: {0000001}, odd parity, P1 = 1) (Hint: 1 111 010 0100)

[3 points]

Question on extended Hamming code

Question: Calculate the final code after encoding the code 11110100100 into 16-bit even parity extended Hamming code. (show your steps, e.g., P1: {0000001}, odd parity, P1 = 1) (Hint: 1 111 010 0100)

[3 points]

(16, 11) Extended Hamming code

data → encoding → codeword

			1
	1	1	1
	0	1	0
0	1	0	0

Lecture 8: Extended Hamming codes

Extended Hamming code is a linear code that can detect and correct single-bit errors, and also detect double-bit errors.

- Uses an extra parity check for the whole block of bits
- For example, parity check on {1100 111 0010 0100}

1	1	1	0
0	1	1	1
0	0	1	0
0	1	0	0

Extended Hamming code (even parity)

Question on extended Hamming code

			1
	1	1	1
	0	1	0
0	1	0	0

Parity: ?

Parity bit at position 1

			1
	1	1	1
	0	1	0
0	1	0	0

Parity: ?

Parity bit at position 2

			1
	1	1	1
	0	1	0
0	1	0	0

Parity: ?

Parity bit at position 4

			1
	1	1	1
	0	1	0
0	1	0	0

Parity: ?

Parity bit at position 8

Question on extended Hamming code

	0		1
	1	1	1
	0	1	0
0	1	0	0

Parity: 0

Parity bit at position 1

P_1: {1110010}
even parity

$P_1 = 0$

(0.6 pts)

	0	0	1
	1	1	1
	0	1	0
0	1	0	0

Parity: 0

Parity bit at position 2

P_2: {1111000}
even parity

$P_2 = 0$

(0.6 pts)

	0	0	1
0	1	1	1
	0	1	0
0	1	0	0

Parity: 0

Parity bit at position 4

P_3: {1110100}
even parity

$P_3 = 0$

(0.6 pts)

	0	0	1
0	1	1	1
0	0	1	0
0	1	0	0

Parity: 0

Parity bit at position 8

P_4: {0100100}
even parity

$P_4 = 0$

(0.6 pts)

Question on extended Hamming code

	0	0	1
0	1	1	1
0	0	1	0
0	1	0	0

Parity: 0

Parity bit at position 0

P_5: {001011100100100}

even parity

$P_5 = 0$

(0.6 pts)

Question: Calculate the final code after encoding the code 11110100100 into 16-bit even parity extended Hamming code. (show your steps, e.g., P1: {0000001}, odd parity, P1 = 1) (Hint: 1 111 010 0100)

Solution: The final code is:

0001 0111 0010 0100

Secure File System Project

Project description and marking guide available on eClass

- Week 6: February 12, 2024
- Same groups of 3 people
- Programming language of your choice (e.g., Python, Java, and C++)
- Following the agile methodology

Final report (6-10 pages)

- Expands on the deliverable, based on the finished product

Demonstration (10-15 minutes)

- After the final report submission, scheduled with the TAs.

Course projects

Project 2: Secure File System

A secure file system that allows its internal users to store data on an untrusted file server.

Project deliverable (10%)

- Due Friday, March 15
- More than two weeks from now

Final report and demo (15%)

- Due Monday, April 8
- Three weeks from the submission of the deliverable

Project deliverable

Project 2: Secure File System Deliverable (3-5 pages)

- Due Friday, March 15

Design

- Class diagram

Tools and technologies

- What technologies you plan to use? Why?

User stories

- Three user stories (persona + need + purpose)
- Each user story should be broken down into sub-tasks

Planning

- Timeline of the subtasks