Review Session I

ECE 422: Reliable and Secure Systems Design

Instructor: An Ran Chen
Term: 2024 Winter

Schedule for today

- Review session I
  - Lecture 17 Encryption - Part I
  - Lecture 19 Encryption - Part II
  - Lecture 20 The Dining Philosophers Problem
  - Lecture 21 Deadlocks
  - Lecture 23 Cookies and Sessions
- SPOT Survey reminder

Format of exam

- Classroom: The Centennial Centre for Interdisciplinary Science (CCIS) 1-160
- Date: Wednesday, Apr 24th, 2024
- Duration: 2 hours
- Closed book
- Materials: all materials posted in the lecture slides
    - => 60% on new materials, < 40% on old materials
- The final counts for 30% of the overall course grade

Email me if you need to know your grade early for work permit or graduation (estimated early grade release date: ~ May 1).

Type of question

- True/False
- Multiple choice
- Short answer
- Essay questions
  - Explain and give examples
- Computational questions
  - Bring your own calculator

List of materials to prepare you

- Go through the concepts in the (midterm + final) review slides
- Go through the questions in the lecture slides

Additional information:

- Materials from the past years: Google Drive link
  - ECE422 W2023 Security in Computing 3 Programs and Programming
  - ECE422 W2023 Security in Computing 4 The Web-User Side
  - ECE422 W2023 Security in Computing 6 Networks
  - ECE422 W2023 Security in Computing 7 Database

Course registration system

User story: As a security admin, I want to ensure the integrity of the data.

- Lecture 13: The CIA Triad
- Lecture 14: Hash function and Digital Signature
    - Hash collision on integrity checks

Key concepts:

- Digital Signature: Authenticity + Integrity + Non-repudiation
- Difference between hashing and encryption: irreversibility

Course registration system

User story: As a web admin, I want to prevent race condition for course registration.

- Lecture 20: The Dining Philosophers Problem
  - Race condition
  - Atomic locking

Key concepts:

- Locks to prevent multiple users from registering the courses at the same time
- Atomic locks for course reservation

Course registration system

User story: As a security admin, I want to ensure the confidentiality of the system.

- Lecture 15: Authentication
  - Multi-factor authentication
- Lecture 16: Access Control
  - Models of access control
- Lecture 17: Encryption
  - Symmetric and asymmetric encryption

Key concepts:

- MFA: knowledge, possession, biologic, location and time
- DAC, RBAC, MAC, ABAC
- Asymmetric: encryption = sender’s private key; decryption = public key

Essay question

Given the following user story written by a portfolio manager or business analyst:

- As a security admin, I want to ensure the confidentiality of the system.

Question: As software developers, how can we implement such a user story?

- Explain confidentiality
- Name an example of technique to ensure confidentiality
- Describe how the technique works
- Explain how it protects the confidentiality

Essay question

Given the following user story written by a portfolio manager or business analyst:

- As a security admin, I want to ensure the confidentiality of the system.

Potential answer:

- Confidentiality is about making sure that only the authorized user has access to particular resources.
- An example of such technique is access control.
- We restrict user access to the system through different models of access control.
- For example, discretionary access control is an identity-based access control model that enforces a security policy based on the identity of the user.

Schedule for today

- Review session I
  - Lecture 17 Encryption - Part I
  - Lecture 19 Encryption - Part II
  - Lecture 20 The Dining Philosophers Problem
  - Lecture 21 Deadlocks
  - Lecture 23 Cookies and Sessions
- SPOT Survey reminder

Security principles

- Lecture 17 Encryption - Part I
  - Rivest–Shamir–Adleman (RSA) algorithm [Problem]
- Lecture 19 Encryption - Part II
  - Diffie-Hellman Key Exchange [Problem]
    - Primitive roots [Problem]
    - Discrete logarithm problem [Explanation]

Question on DF algorithm

Suppose that Alice and Bob want to agree on a shared "secret key" with p = 11 and g = 2.

Question: If Alice chooses 9 and Bob chooses 4 as their respective secret integers, what are their public integers and what is their secret key? (show the calculations for both Alice and Bob)

- $A = g^a \ mod(p)$
- $B = g^b \ mod(p)$
- $K = g^{ab} \ mod(p) = A^b \ mod(p)$
- $K = g^{ba} \ mod(p) = B^a \ mod(p)$

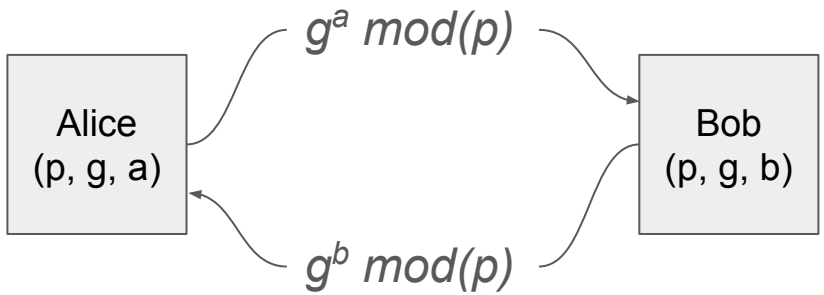
Question on DF algorithm

Suppose that Alice and Bob want to agree on a shared "secret key" with p = 11 and g = 2.

Question: If Alice chooses 9 and Bob chooses 4 as their respective secret integers, what are their public integers and what is their secret key? (show the calculations for both Alice and Bob)

Thought process: We have the values p, g, a and b, asked to calculate A, B, K

- We need to calculate A, B to find K
  - Step 1: calculate the public integers
  - Step 2: calculate the secret key
    - Bob uses $K = A^b \ mod(p)$
    - Alice uses $K = B^a \ mod(p)$

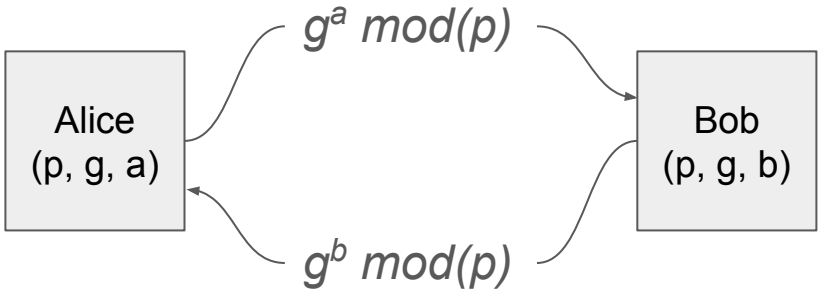


Question on DF algorithm

Solution: We have the values p, g, a and b, asked to calculate A, B, K

Step 1: calculate the public integers

- A = $g^a \ mod(p)$ = 2^9 mod (11) = 6
- B = $g^b \ mod(p)$ = 2^4 mod (11) = 5



Step 2: calculate the secret key

- For Bob, $K = A^b \ mod(p)$ = 6^4 mod (11) = 9
- For Alice, $K = B^a \ mod(p)$ = 5^9 mod (11) = 9

Question on DF algorithm

Suppose that Alice and Bob want to agree on a shared "secret key" with p = 11 and g = 2.

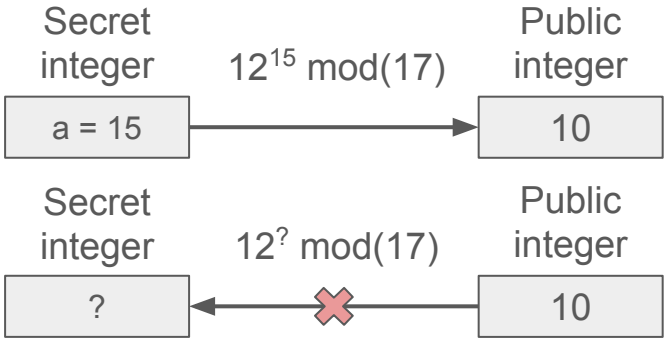
Question: If Alice chooses 9 and Bob chooses 4 as their respective secret integers, what are their public integers and what is their secret key? (show the calculations for both Alice and Bob)

In real-life scenario, much larger values of a, b and p are required. An eavesdropper cannot discover the shared secret key even if she knows p and g and can obtain the public integers.

Discrete Logarithm Problem (DLP)

For Eve to find the secret integer, she needs to solve the discrete logarithm problem, however

- It is easy to calculate the public integer
- Hard to find the secret integer (many solutions)



The idea is similar to the shared secret color solution:

- Easy to mix a secret color with the starting one to get a mixture
- Hard to find the secret color from the mixed color (many color combinations)

Primitive roots

Question: Is 3 a primitive root of prime number 7?

Answer: Yes, 3 is a primitive root of 7.

- For every integer coprime to 7, there is a power of 3 that is congruent.
- Integers that are coprimes to 7: 1, 2, 3, 4, 5, 6
- $3^1 \bmod(7) = 3$
- $3^2 \bmod(7) = 2$
- $3^3 \bmod(7) = 6$
- $3^4 \bmod(7) = 4$
- $3^5 \bmod(7) = 5$
- $3^6 \bmod(7) = 1$
- Verified: For 1, 2, 3, 4, 5, 6, there is a power of 3 that is congruent

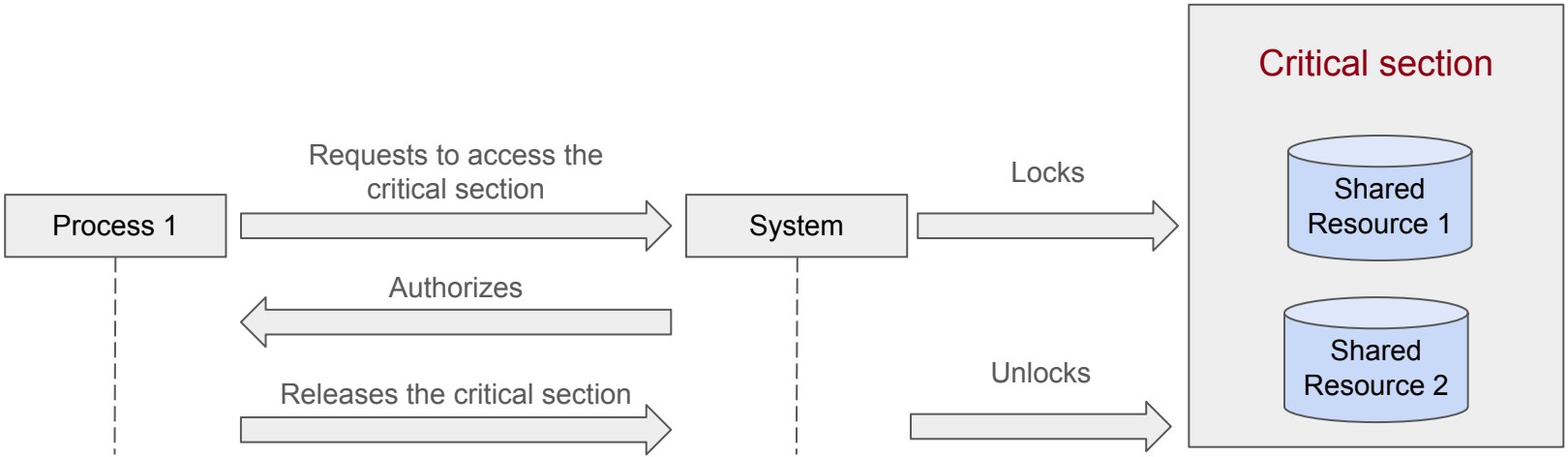
Reliable design

- Lecture 20 The Dining Philosophers Problem
  - Deadlocks vs starvation
  - Deadlock prevention (mutual exclusion, hold and wait, no preemption, circular wait)
  - Prevent circular wait: atomic locks on critical section [Explanation]
    - Locking mechanism: Race condition
    - Atomic property: Deadlocks
- Lecture 21 Deadlocks
  - Deadlock avoidance: Resource Allocation Graph (RAG) [Problem]
  - Banker's Algorithm = Resource Allocation Table

Solution: atomic locking

Introducing atomic locks to the resources:

- Ensure that the resource is accessed by only one process at a time
- If the lock is free, the system will allow the process to access the resources and lock the critical section

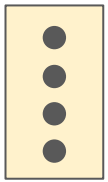


Resource Allocation Graph (RAG)

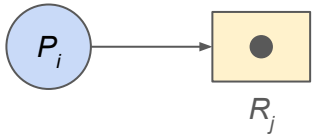
- P_i, Process

- R_j, Resource with instances
  - Resource with a single instance

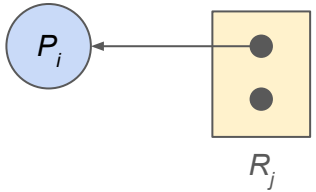
  - Resource with 4 instances



- P_i requests instance of R_j

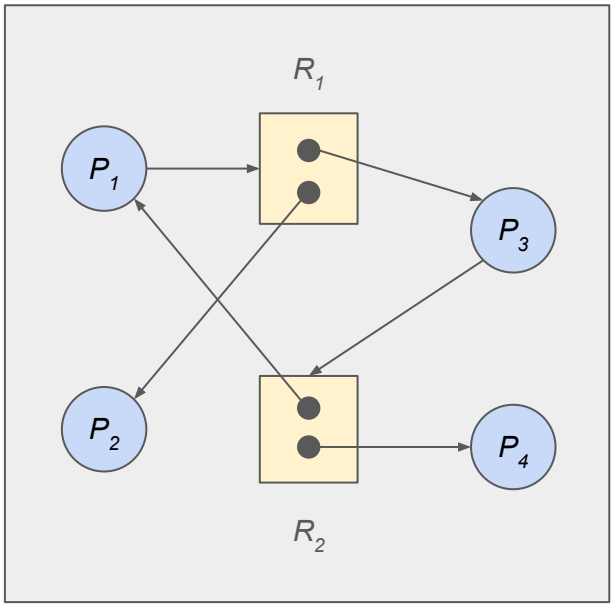


- P_i is holding an instance of R_j



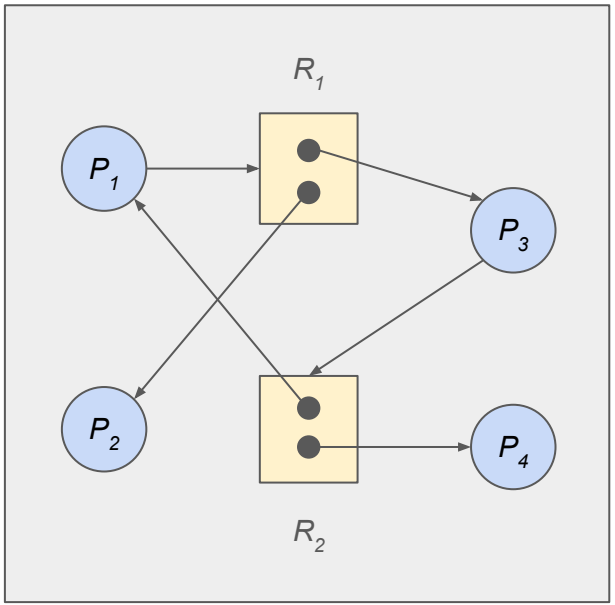
Question on RAG

Question: Based on the following RAG, is there a deadlock?



Question on RAG

Question: Based on the following RAG, is there a deadlock?

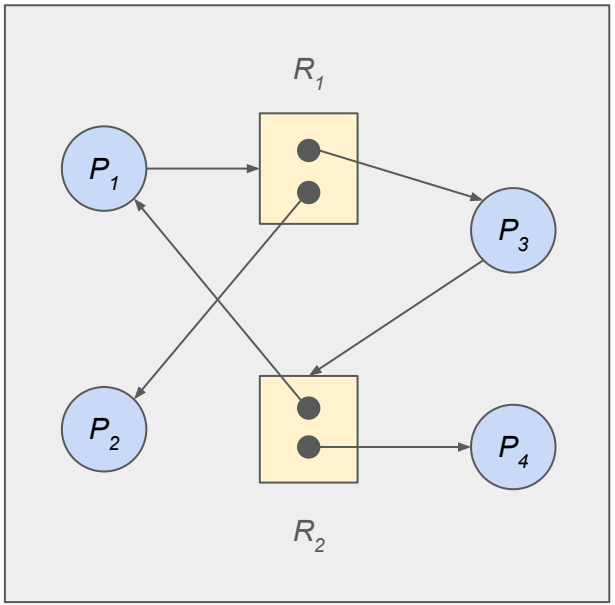


Thought process: Perform two checks. If neither of them indicates there is a deadlock, then solve the resource allocation table.

- Cycle check
  - If none, then no deadlock
- Single instance check
  - If only one instance per resource, then deadlock
- Solve the resource allocation table

Question on RAG

Question: Based on the following RAG, is there a deadlock?

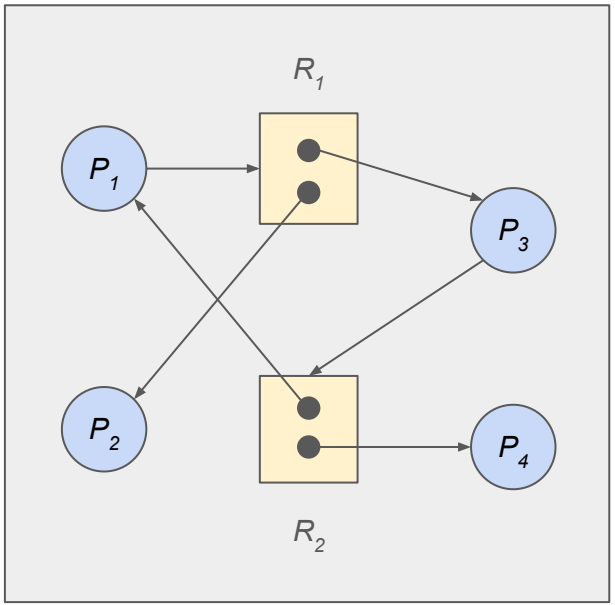


Step 1: Perform two checks

- Cycle check
  - Yes, P1 → R1 → P3 → R2 → P1
- Single instance check
  - R1 and R2: more than one instance
- Solve the resource allocation table

Question on RAG

Question: Based on the following RAG, is there a deadlock?



Step 2: Solve the resource allocation table

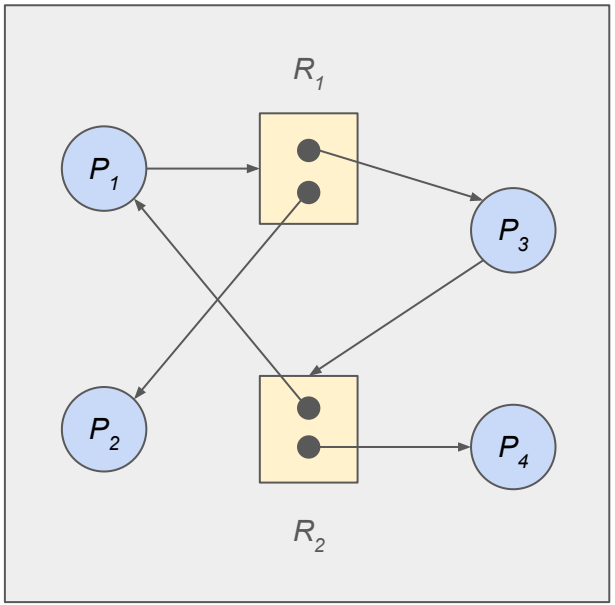
- Fill in the allocated/requested resources

	Allocated		Requested	
	R1	R2	R1	R2
P1				
P2				
P3				
P4				

Hint: allocated = R → P; requested = P → R

Question on RAG

Question: Based on the following RAG, is there a deadlock?



Step 2: Solve the resource allocation table

- Fill in the allocated/requested resources

	Allocated		Requested	
	R1	R2	R1	R2
P1	0	1	1	0
P2	1	0	0	0
P3	1	0	0	1
P4	0	1	0	0

Hint: allocated = R → P; requested = P → R

Question on RAG

Question: Based on the following RAG, is there a deadlock?

	Allocated		Requested	
	R1	R2	R1	R2
P1	0	1	1	0
P2	1	0	0	0
P3	1	0	0	1
P4	0	1	0	0

Step 3: Free the requested resources

- Availability = (R1, R2) = (0, 0)
- Availability = (1, 0) after P2
- Availability = (1, 1) after P4
- Availability = (1, 1) after P3

Cycle with no deadlock

Question on RAG

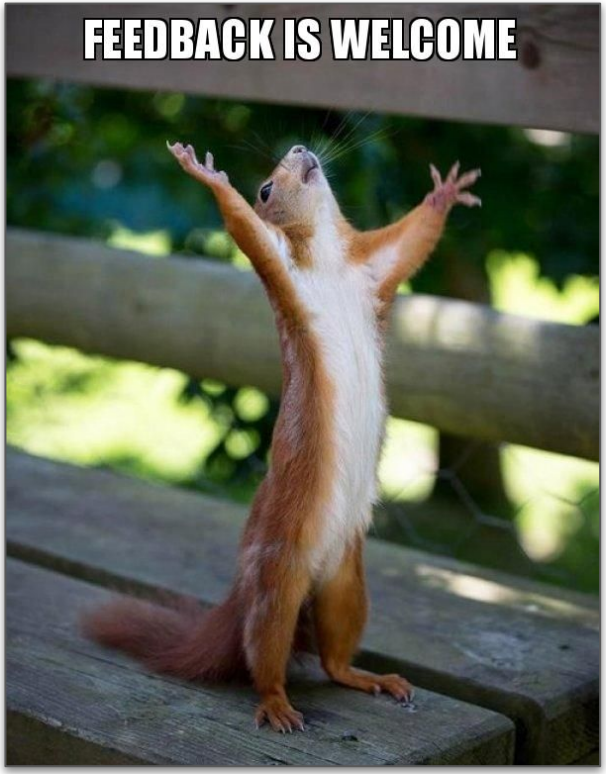
Question: Based on the following resource allocation, is there a deadlock (draw RAG)?

- Suppose that there are two resources (R1 and R2), each with two instances
- P1 allocates an instance of R2, and requests an instance of R1
- P2 allocates an instance of R1
- P3 allocates an instance of R1 and requests an instance of R2
- P4 allocates an instance of R2

Security principles

- Lecture 23 Cookies and Sessions
  - Ambient authority (cookies, IP checking, certificates, basic authentication)
  - Session cookies
  - Cookie protections
    - Signing cookies [Explanation]
      - Session fixation attack
    - Cookie attributes [Explanation]

SPOT Survey



SPOT Survey: Click here

- 15 minutes
- Course number: 15754
- Survey close: Apr 14, 11:59 PM

If we can just get 5 more students completing the survey, I will have the final exam graded within a week (May 1st) and […]