SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

CMPT 300: Operating Systems I

Assignment 4

Due July 31, 2018

POLICIES:

1. **Coverage**
   Chapters 10-15
2. **Grade**
   10 points, 100% counted into the final grade
3. **Individual or Group**
   Individual based, but group discussion is allowed and encouraged
4. **Academic Honesty**
   Violation of academic honesty may result in a penalty more severe than zero credit for an assignment, a test, and/or an exam.
5. **Submission**
   Electronic copy via CourSys
6. **Late Submission**
   2-point deduction for late submission within one week;
   5-point deduction for late submission over one week;
   Deduction ceases upon zero;
   Late submissions after the sample solution is available will NOT be graded.

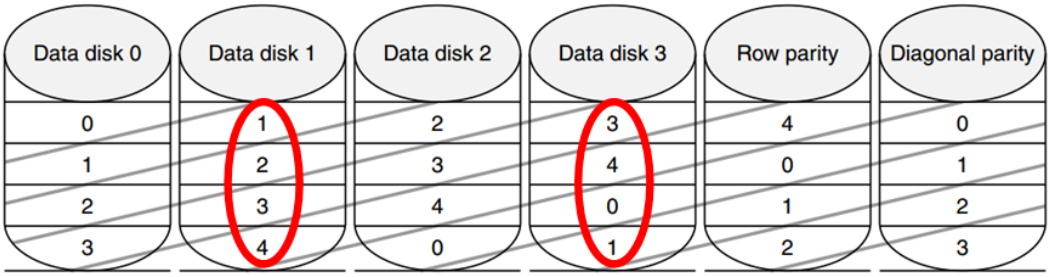
QUESTIONS:

1. **1 point**
   Assume the following RAID 3 system uses ODD parity and disk2 fails.

Disk 1	Disk 2 - Failed	Disk 3	Parity
1		1	1
0		0	1
1		1	0
0		0	0
0		0	1
0		0	1
1		1	0
1		1	1

a. Determine the original data on disk 2 and fill in the form.
b. Use the first two rows as example to explain how the original data is recovered.
[Grading Rubric: 1 point if both subquestions are correctly answered.]

2. **1 point**
Provide a suitable recovery sequence for the illustrated RAID-DP (or row-diagonal parity) with disks 1 and 3 failed.



[Grading Rubric: 1 point if a correct recovery sequence is provided. 0 point otherwise.]

3. **2 points**
Suppose that a disk drive has 5,000 cylinders, numbered through 0 to 4,999. The drive is currently serving a request at cylinder 2,150, and theprevious request was at cylinder 1,805. The queue of pending requests, in FIFO order, is:
2,069, 1,212, 2,296, 2,800, 544, 1,618, 356, 1,523, 4,956, 3,681

Starting from the current head position, what is the total distance (in cylinders) that the disk arm moves to satisfy all the pending requests for each of the following disk-scheduling algorithms?
a. FCFS
b. SSTF
c. SCAN
d. LOOK
e. C-SCAN
f. C-LOOK
[Grading Rubric: 2 points if ALL sixed distances are correctly calculated.
1 point if at least three distances are correctly calculated. 0 point otherwise.]

4. **1 point**
How does DMA increase system concurrency?
[Grading Rubric: Derivation of the correct result should be provided.]

5. **1 point**
What is the purpose of using a "salt" along with the user-provided password?
[Grading Rubric: Both the limitation of password designs without salts and

the benefit of using salts should be discussed.]

6. **2 points**

   a. What is the key difference between symmetric encryption and asymmetric encryption?

   b. What is the key difference between a message-authentication code and a digital signature?

   [Grading Rubric: 1 point per subquestion.]

7. **2 points**

   Consider a time-consuming authentication scenario where a database records all secret keys of a large number of users. When the system authenticates a user, it first issues a challenge message to the user. The user then uses his/her key to encrypt the challenge and then returns the encrypted challenge to the system. The system then encrypts the challenge using one key in the database after another and compares the result with the received encryption. Once a match is found, the system accepts the user. Otherwise, the user is denied. This authentication protocol surely takes a lot of time and computation.

   Design a possible solution to speed up the authentication process.

   [Grading Rubric: Open question, again! Time to convince the TA.
   If you consider such questions interesting, join a research lab.
   Finally, the last question of the last assignment of CMPT 300. Enjoy.]