Final Exam

Mengxiang Jiang
CSEN 5322 Operating Systems

December 3, 2022

Problem 1. Assume p and q are two large prime number - what are the steps in RSA algorithm to form a private key as well as a public key?

1. Choose large prime numbers p and q
2. Compute the product $n = p \times q$ and the product $z = (p-1) \times (q-1)$
3. Choose a number relatively prime to z and call it d
4. Find e such that $e \times d \equiv 1 \pmod{z}$
5. To encrypt a message P, compute $C \equiv P^e \pmod{n}$.
   To decrypt C, compute $P \equiv C^d \pmod{n}$

Problem 2. Consider a swapping system in which memory consists of the following hole sizes in memory order: 10 KB, 4 KB, 20KB, 18 KB, 7 KB, 9 KB, 12 KB, and 15 KB. Which hole is taken for successive segment request of 12 KB, 10 KB and 9 KB, for (a) first fit, (b) best fit, (c) worst fit and (d) next fit

(a) first fit:

segment	12 KB	10 KB	9 KB
hole	20 KB	10 KB	18 KB

(b) best fit:

segment	12 KB	10 KB	9 KB
hole	12 KB	10 KB	9 KB

(c) worst fit:

segment	12 KB	10 KB	9 KB
hole	20 KB	18 KB	15 KB

Problem 3. (a) Suppose that two strangers A and B want to communicate with each other using secret-key cryptography, but do not share a key. Suppose both of them trust a thirdparty C whose public key is well known. How can the two strangers establish a new shared secret key under these circumstances? (b) In the UNIX password system, what is salt and how does it help defeat password cracking?

(a) A can use public key cryptography sytem (like RSA) to communicate a secret key to C and have C also use the public key system to communicate A's secret key to B.

(b) Salt is an additional randomly generated string that's concatenated to a user's password before hashing. It only defends against dictionary attacks on all users rather than a targeted attack on a single user, since now crackers who knows a lot of passwords but not the user they belong to cannot simply perform hashing and compare the password hashes.

Problem 4. (a) RAID level 3 is able to correct single bit errors using only one parity drive. What is the point of RAID level 2? After all, it also only correct one error and takes more drives to do so. (b) Mention one advantage of hard links over symbolic links and advantage of symbolic links over hard links.

(a) RAID 2's Hamming code can pinpoint exactly which bit errored while RAID 3 does not (in practice disks can often know its malfunctioning due to checksums so RAID 3's error detection is correlated to error correction but not strictly equivalent)

(b) Soft/symbolic links can link to files on remote computers as well as directories while hard links can only link to files on the same computer. Hard links however still exists even if you delete, move, or rename the original file while symbolic/soft links become meaningless.

Problem 5. How many disk operations are needed to fetch the i-node for the file */usr/uno/courses/os/slide*7*.ppt*? Assume that the i-node for the root directory is in memory, but nothing else along the path is in memory. Also, assume that all directories fit in one disk block.

directory for /
i-node for /usr
directory for /usr
i-node for /usr/uno
directory for /usr/uno
i-node for /usr/uno/courses
directory for /usr/uno/courses
i-node for /usr/uno/courses/os
directory for /usr/uno/courses/os
i-node for /usr/uno/courses/os/slide7.ppt
Total 10 disk reads.

Problem 6. What is a journaling file system and what is it used for?

Journaling keeps a log of the transaction to be performed on a disk write. This allows recovery of the file system in case of a crash or power outage by retrying incomplete transactions.

Problem 7. Consider a disk where seek time dominates rotational latency and transfer time. Hence, we only care about how many tracks need to seek over to service our requests. Cylinders on the disk are numbered from 0 (innermost) to 20 (outermost). The disk head currently resides on cylinder 8. Consider the start of servicing disk request to be time 0. Count time in number of seeks and calculate the number of seeks required to service the following requests under the given scheduling algorithms. Also calculate the average seek time per request.

REQUEST NAME	REQUEST ARRIVES	CYLINDER REQUESTED
A	after 0 seeks	12
B	after 0 seeks	4
C	after 0 seeks	10
D	after 0 seeks	2
E	after 8 seeks	20
F	after 8 seeks	3
G	after 8 seeks	17
H	after 14 seeks	4

Use (a) Shortest Seek First (SSF) algorithm and (b) Elevator algorithm (SCAN), considering the initial movement of the disk head to go inward from cylinder 8.

(a) shortest seek first:

name	C	A	B	F	D	H	G	E
required time	2	2	8	1	1	2	13	3
total time	2	4	12	13	14	16	29	32

average time = 32/8 = 4

(b) elevator:

name	B	D	C	A	G	E	H	F
required time	4	2	8	2	5	3	16	1
total time	4	6	14	16	21	24	40	41

average time = 41/8 = 5.125