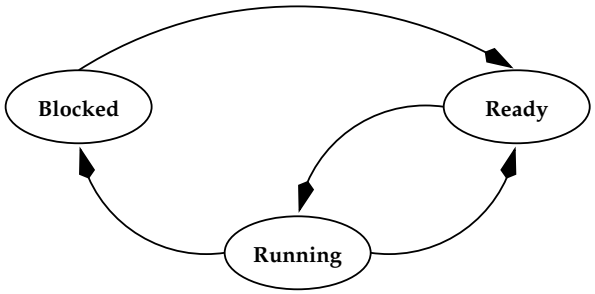
Introduction to Operating Systems
Final Examination

Name:_____ E-mail:_____

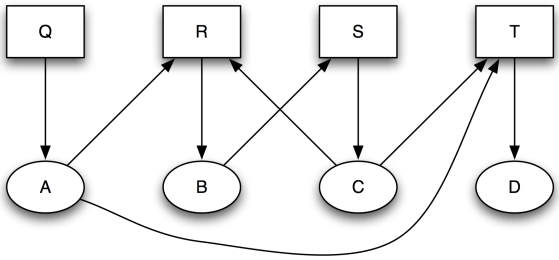
Winter 2015

There are fifteen questions in this examination (and one *extra credit* question). All have equal weight. Answer them clearly and *concisely* (hot air is worth *zero* points, and *unnecessary bloviation* may result in a reduction in points). All questions require *at most* a short answer (a few sentences).

1. Label each of the transitions in the following process state diagram and in *one* sentence say what causes each to be made.



2. Consider the following resource graph. Which processes (A, B, C, D) and which resources (Q, R, S, T) are deadlocked? What needs to be done to break the deadlock? Briefly explain how you knew that.



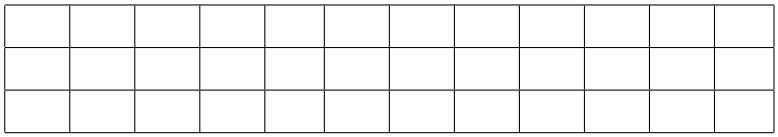
3. Deadlock can be prevented by negating (making impossible) any one of four necessary and sufficient conditions (Coffman 1971). Briefly define each of these conditions.

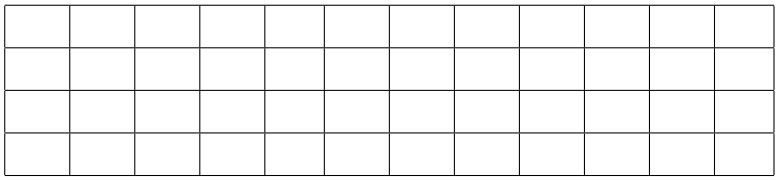
4. Given that you have a RAID-4 system composed of five disks, fill in the formula for $P = \_\_\_ \oplus \_\_\_ \oplus \_\_\_ \oplus \_\_\_$ and for $D_1 = \_\_\_ \oplus \_\_\_ \oplus \_\_\_ \oplus \_\_\_$. Now, suppose that D_3 fails, give the formula for D_3 and briefly list the steps for reconstructing its data.

5. Briefly describe the *Clock* page replacement algorithm.

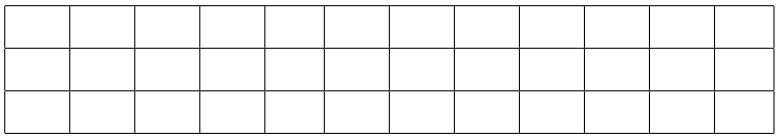
6. The LRU page replacement algorithm has the property that for memory $\mathcal{M}$ of capacity m and a reference string r, $\mathcal{M}(r, m) \subseteq \mathcal{M}(r, m+1)$. What is this property called and why does this preclude LRU from suffering Belady's anomaly? What exactly is *Belady's anomaly*?

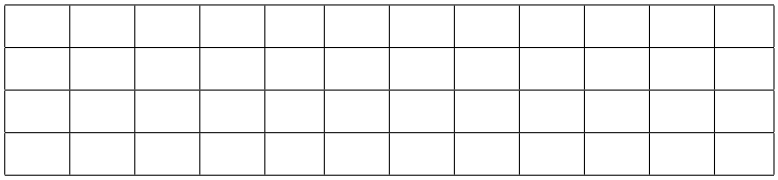
7. Using the reference string $\langle 2\ 4\ 3\ 8\ 2\ 4\ 7\ 2\ 4\ 3\ 8\ 7 \rangle$, fill in the two tables below (representing *three* and *four* page frames) using the FIFO page replacement policy. How many page faults occur?





Now do the same thing for LRU.





8. Describe (it will help if you draw a picture) how *i-nodes* are used to locate the blocks making up a file.

9. Suppose that you have a UNIX file system where the disk block size is 1 kB, and an *i*-node takes 64 bytes. Disk addresses take 32 bits, and the *i*-node contains 8 direct addresses, one indirect, one double-indirect and one triple-indirect (the rest of the space in the *i*-node is taken up with other information). An index block is the same size as a disk block.

   Suppose you write one byte each at offsets $0, 1024, 65539\ (2^{16}+3)$, and $1048577\ (2^{20}+1)$. How much total disk space does the file consume (including overhead)?

   n.b. Think carefully before you rush to answer this question, there is a subtlety you might miss.

10. Give a simple protocol that will allow *Alice* to share with *Waldo* a value x such that Waldo knows that only Alice could have sent it, and Alice knows that Waldo received it. Using the notation $A \to W : \mathcal{E}_A(x)$, which means "Alice sends x to Waldo encrypted with her *public* key" and $W \to A : \mathcal{D}_W(y)$, which means "Waldo sends y to Alice encrypted with his *private* key."

11. An RSA (Rivest-Shamir-Adelman) cryptosystem is composed of $e, d, n = pq$ and where $d \times e \equiv 1 \bmod \varphi(n)$. The public key is e, the private key is d, n is also public but p, q and $\varphi(n)$ are private.

    (a) $n =$ _____ and $\varphi(n) =$ _____.

    (b) If the adversary can discover p or q, the formula for computing d is _____.

    (c) The formula for $\mathcal{E}(m) =$ _____ and for $\mathcal{D}(c) =$ _____.

    (d) Why is it safe for n to be made public?

12. *Capabilities* have two well-known problems: the *capability propagation problem* and the *capability revocation problem*. In a few sentences (at most), describe both of these problems.

13. In order to use an *access control list* in a distributed system, a process must prove its _____.

14. Suppose that you have a clock chip that operating at 3 MHz, that is, three times per microsecond the clock will subtract one from a counter. When the counter reaches zero, an interrupt occurs. The counter is 16 bits. What value do you use to reset the counter? Use **C**-like pseudocode to show how to implement a *time of day clock.*

15. If we do not trust a program then we must attempt to confine it. But, confinement is difficult since there can be covert channels for leaking information. Give a simple example of a covert channel that a malevolent program might use to leak information.

16. **Extra Credit** (replaces lowest scored question).

    A Diffie-Hellman key exchange requires a base a, and a prime p. A must choose an x and B must choose a y. It then proceeds as follows:

$$\begin{aligned} A \rightarrow B: &\quad a, p, a^x \pmod p \\ B \rightarrow A: &\quad a^y \pmod p \end{aligned}$$

    (a) What secret do A and B now share?

    (b) Why doesn't the adversary also know this secret?

    (c) What would be necessary for the adversary to learn this secret?