Answer sheet for CS 136 Midterm Exam, Spring 2009

Multiple choice questions

1.	a
2.	c
3.	b
4.	d
5.	a
6.	d
7.	a
8.	c
9.	b
10.	c
11.	c
12.	b
13.	d
14.	c
15.	d
16.	a
17.	a
18.	b
19.	a
20.	d

Short Answer questions

1. Because the entity that can provide actual access control isn't the entity that originated the policy. It's especially hard in distributed systems, since the supposedly controlled data may move away from systems that can be trusted to follow the originator's policy.
2. Each step in the task should be assigned to the same Conflict of Interest class. Once a subject has performed one of the tasks, the Chinese wall policy will prevent him from performing any of the others, since they're in the same COI class.
3. DES is easier, because it makes use of simple arithmetic and logical operations that are easy to implement in hardware. RSA uses exponentiation, which is not easy to implement in hardware.
4. The other authorities might be untrustworthy, in which case they might provide the number to subjects who should have had their access revoked. Even if the capability is protected cryptographically, unless it's tied to the particular subject, the untrustworthy remote system might give a copy to the wrong party.
5. The advantage is that a password not in any actual dictionary might be used, while still being relatively easy to remember. The disadvantage is that brute force attacks need only test all legal combinations of phonemes, not all legal combinations of letters, making the attack a lot easier.