University of Washington
Department of Computer Science and Engineering
CSE 321, Winter 2008

February 8, 2008

Midterm Exam, Friday, February 8, 2008

NAME: ____________________________

Instructions:

- Closed book, closed notes, no cell phones, no calculators.
- Time limit: 50 minutes.
- Answer the problems on the exam paper.
- If you need extra space use the back of a page.
- Problems are not of equal difficulty, if you get stuck on a problem, move on.

1	/10
2	/20
3	/10
4	/15
5	/10
6	/10
7	/10
Total	/85

Problem 1 (10 points):

a) Show that the expression $(p \to q) \to (p \to r)$ is a contingency.

b) Give an expression that is logically equivalent to $(p \to q) \to (p \to r)$ using the logical operators $\neg$, $\vee$, and $\wedge$ (but not $\to$).

Problem 2 (20 points):

Using the predicates:

$\mathit{Likes}(p, f)$: "Person p likes to eat the food f."

$\mathit{Serves}(r, f)$: "Restaurant r serves the food f."

translate the following statements into logical expressions.

a) Every restaurant serves a food that no one likes.

b) Every restaurant that serves TOFU also serves a food which RANDY does not like.

Translate the following logical expressions into English. (You may want to give a couple of sentences of explanation - the point of this question is to demonstrate that you understand the logical expression.)

c) $\exists r \forall p \exists f (\mathit{Serves}(r, f) \wedge \mathit{Likes}(p, f))$

d) $\forall r \exists p \forall f (\mathit{Serves}(r, f) \to \mathit{Likes}(p, f))$

Problem 3 (10 points):

Determine the value of the following. (You will probably want to use different methods to compute the values.)

a) $3^{303} \bmod 101$

b) $3^{64} \bmod 100$

Problem 4 (15 points):

a) What is public key cryptography?

b) What is the computation that "Alice" employs when she encodes a message using RSA?

c) Why is RSA considered secure?

Problem 5 (10 points):

Use rules of inference to show that if the premises $\forall x(P(x) \rightarrow Q(x))$, $\forall x(Q(x) \rightarrow R(x))$, and $\neg R(a)$, where a is in the domain, are true, then the conclusion $\neg P(a)$ is true. (Note: You do not need to give the names for the rules of inference.)

Problem 6 (10 points):

Prove that if n is even and m is odd, then $(n+1)(m+1)$ is even.

Problem 7 (10 points):

Prove or disprove:

a) For positive integers x, p, and q, $(x \bmod p) \bmod q = x \bmod pq$.

b) For positive integers x, p, and q, $(x \bmod p) \bmod q = (x \bmod q) \bmod p$.