Instructions:

1. This exam is a closed-book, closed-notes exam.

2. **Legibility counts!** Make sure I can read (and find!) your answers.
   If you need more room for an answer than that given, use the back side of the pages. Be sure to leave a note indicating where the answer is.

3. This test should have 8 pages (including this cover sheet). Let me know now if your copy does not have the correct number of pages.
1. (20 points) Consider the following plausible inference rule:

\[
\begin{array}{c}
P \text{ reps } Q \text{ on } \varphi \\
Q \Rightarrow R \\
\hline
P \text{ reps } R \text{ on } \varphi
\end{array}
\]

Determine whether or not this rule is *sound*, and justify your answer as follows:

- If you determine that the rule is sound, prove its soundness.
- If you determine that the rule is not sound, give (and explain!) a particular Kripke structure, principals \(P, Q, R\) and formula \(\varphi\) that demonstrate the lack of soundness.
2. (14 points) Van and Ray have decided to get married and have headed to the county clerk’s office to obtain a marriage license. The rules that govern marriage licenses in their locale are as follows:

- Both parties must appear in person to request a marriage license.
- Both individuals must provide government-issued photo identification, such as a driver’s license or a passport.

For the purposes of this question, let \( \langle \text{license, Van, Ray} \rangle \) represent the proposition “it is a good idea to issue a marriage license to Van and Ray.”

Answer the following questions regarding the relevant certifications, credentials, and access-control policies needed for Van and Ray to obtain their marriage license. All your answers should be expressions in the access-control logic.

(a) Van and Ray show up in person at the county clerk’s office and request a marriage license. What is the form of this request? (Note: The county clerk has never met either of them prior to their arrival at the office.)

(b) For identification purposes, Van presents a driver’s license issued by the New York Department of Motor Vehicles (DMV), and Ray presents a Canadian passport. Express these identification certificates as expressions in the logic.

(c) What are the additional certificates, authorizations, recognition of authority, and trust assumptions that are necessary for the county clerk’s office to grant marriage license to Van and Ray?
3. (26 points) A small restaurant has installed a PKI-enabled electronic register to track food orders as well as billing. The relevant workings of this register are as follows:

- The manager’s (Don) key pair is \((K_D, K_D^{-1})\), and his public key is directly installed on the machine.
- Don assigns/certifies key pairs to all employees: Cara’s key pair is \((K_C, K_C^{-1})\), and Ellis’s key pair is \((K_E, K_E^{-1})\).
- Before each shift begins, Don uses his private key to log into the system and to enter the table assignments for each of the waitstaff.
  Table assignments are treated as delegations: a member of the waitstaff places food orders on behalf of the table(s) to which they are assigned.
- To place food orders into the system on behalf of customers (i.e., tables), members of the waitstaff must log in with their own private keys.

For this morning’s shift, Don assigned Table 5 to Cara, which means that she is the authorized representative/delegate for placing food orders on behalf of Table 5.

Let the propositional variable \(\langle \text{order}, \#5 \rangle\) denote the action of placing a food order for Table 5 into the system.

Answer the following questions regarding the certifications, credentials, and access-control policies needed for the electronic register. All your answers should be expressions in the access-control logic.

(a) What is the access policy associated with placing food orders for Table 5 into the register?

(b) What is the delegation certificate that reflects Cara’s table assignment?

(c) Later in the day, Cara waits on a customer at Table 5. What is the form of the request when she attempts to place the order into the register?

(d) What are the additional certificates, recognition of authority, and trust assumptions regarding keys that are necessary for the electronic register to determine that the food order should be accepted?
(e) Don cannot be at the restaurant all the time, so he has configured the system to allow his assistant manager (Ellis) to make table assignments on his behalf. Specifically, Don has signed a delegation certificate enabling Ellis to sign table-assignment certificates on his behalf. What is the form of this delegation certificate, as it relates to assigning Cara to Table 5?

(f) One day, in Don’s absence, Ellis elects to assign Cara to Table 5. What is the delegation certificate that corresponds to Cara’s table assignment in this case?

(g) What are the additional certificates, recognition of authority, and trust assumptions regarding keys that are necessary for the electronic register to determine that Cara really is Table 5’s delegate. You do not need to include any assumptions already included in part (d).
Syllogism

Speaks For terms of set intersection:

to go outside.

Thus, returning to Example 2.7,

For example, if

the interpretation function

A formal proof of

Some useful derived rules

Conjunction ϕ₁ ϕ₂
ϕ₁ ∧ϕ₂
Simplification (1) ϕ₁ ...
Assumption
2. ϕ₂ Assumption
3. ϕ₁ ⊃ (ϕ₂ ⊃ (ϕ₁ ∧ϕ₂)) Taut
4. ϕ₂ ⊃ (ϕ₁ ∧ϕ₂) 1,3 Modus Ponens
5. ϕ₁ ∧ϕ₂ 2,4 Modus Ponens

Disjunction (1) ϕ₁
ϕ₁ ∨ϕ₂
Disjunction (2) ϕ₂
ϕ₁ ∨ϕ₂

Modus Tollens ϕ₁ ⊃ ϕ₂
¬ϕ₂
ϕ₁
Double negation ¬¬ϕ
ϕ

Disjunctive Syllogism ϕ₁ ∨ϕ₂
¬ϕ₁
ϕ₂

Hypothetical Syllogism ϕ₁ ⊃ ϕ₂
ϕ₂ ⊃ ϕ₃
ϕ₁ ⊃ ϕ₃

Controls P controls ϕ P says ϕ

Derived

P ⇒ Q P says ϕ
Q says ϕ

Derived

P ⇒ Q Q controls ϕ
P controls ϕ

Says

P says (ϕ₁ ∧ϕ₂)
P says ϕ₁

Says

P says (ϕ₁ ∧ϕ₂)
P says ϕ₂

Simplification (1)
**FIGURE 3.1** Logical rules for the access-control logic

### Taut
\[ \varphi \]
if \( \varphi \) is an instance of a prop-logic tautology

### Modus Ponens
\[ \frac{\varphi, \varphi \supset \varphi'}{\varphi'} \]
Says \( P \) says \( \varphi \)

### MP Says
\[ (P \text{ says } (\varphi \supset \varphi')) \supset (P \text{ says } \varphi \supset P \text{ says } \varphi') \]

### Speaks For
\[ P \Rightarrow Q \supset (P \text{ says } \varphi \supset Q \text{ says } \varphi) \]

### & Says
\[ (P \& Q \text{ says } \varphi) \equiv ((P \text{ says } \varphi) \& (Q \text{ says } \varphi)) \]

### Quoting
\[ (P \mid Q \text{ says } \varphi) \equiv (P \text{ says } Q \text{ says } \varphi) \]

### Idempotency of \( \Rightarrow \)
\[ P \Rightarrow P \]

### Transitivity of \( \Rightarrow \)
\[ \frac{P \Rightarrow Q \quad Q \Rightarrow R}{P \Rightarrow R} \]

### Monotonicity of \( \Rightarrow \)
\[ \frac{P \Rightarrow P' \quad Q \Rightarrow Q'}{P \mid Q \Rightarrow P' \mid Q'} \]

### Equivalence
\[ \frac{\varphi_1 \equiv \varphi_2 \quad \psi[\varphi_1/q]}{\psi[\varphi_2/q]} \]

### \( P \) controls \( \varphi \)
\[ \overset{\text{def}}{=} (P \text{ says } \varphi) \supset \varphi \]

**FIGURE 3.2** Common propositional-logic tautologies

\[
\begin{align*}
p \lor \neg p & \quad p \supset (q \supset (p \land q)) \\
p \equiv (\neg \neg p) & \quad (p \land q) \supset (p \supset q) \\
p \supset (q \lor p) & \quad (p \land q) \supset (q \land p) \\
p \supset (q \supset p) & \quad (p \equiv q) \supset (p \supset q) \\
(p \land q) \supset p & \quad ((p \lor q) \land \neg p) \supset q \\
\neg (\neg p \land p) & \quad ((p \supset q) \land (q \supset r)) \supset (p \supset r)
\end{align*}
\]
FIGURE 7.1 Logical Rules for Delegation

\[ P \text{ reps } Q \text{ on } \varphi \; \text{def} = \; P \mid Q \text{ says } \varphi \supset Q \text{ says } \varphi \]

\[ \text{Reps} \; Q \text{ controls } \varphi \; P \text{ reps } Q \text{ on } \varphi \; P \mid Q \text{ says } \varphi \]

\[ \varphi \]

\[ \text{Rep Controls} \; A \text{ reps } B \text{ on } \varphi \equiv (A \text{ controls } (B \text{ says } \varphi)) \]

\[ \text{Rep Says} \; A \text{ reps } B \text{ on } \varphi \; A \mid B \text{ says } \varphi \]

\[ B \text{ says } \varphi \]