**Homework Week01**

**Circularity (1 mark)**

What is the answer to this question?

*Answer:*

Leslie Lamport's pants

**Dining Cryptographers (2 marks)**

Assume the setting described in the first lecture for the problem of the Dining Cryptographers. Suppose we modify the protocol so that paying cryptographers now tell the truth about whether the coin tosses are different or equal. Instead, they will lie about whether they got head or tails.

At the end, do we still know if the NSA paid or not? Is confidentiality still preserved? Briefly explain why or why not.

*Answer:*

⊤ (truth) to model “different”, heads

⊥ (falsity) to model “equal”, tails

*Claim:*

iff there's an odd number of diffs

iff there's an even number of diffs

*Case 1: Suppose NSA paid*

*Case 2: Suppose one of us paid (C1 paid)*

*Therefore:*

It can prove that an odd number of “diff.” means the NSA paid. An even number of “diff.” means one of the *Ci* paid.

**Safety and Liveness (5 marks)**

**Limit closures**

Let  be a state, and let  denote the behaviour (i.e. infinitely many repetitions of .)

Give an example of a set  such that , but

*Answer:*

When set A is a liveness property and no finite prefix of ever fulfills the promise of the liveness property.

**Alpern and Schneider's theorem**

1. Let . That is, we assume there are only two states,  and . Consider the property . Use Alpern and Schneider's theorem to decompose  into a safety property  and a liveness property . Simplify them; that is, don't just say  but give something that explains what  is.
2. Assume  is a safety property. Prove that  using the algebraic laws of set operations.
3. Is the empty property  a liveness property? Is it a safety property? Explain.

*Answer:*

*1.*

*2.*

3.

**Temporal Logic (5 marks)**

**Examples**

Define suitable predicate symbols and give LTL formalisations for the following properties:

1. Once the dragon was slain, the princess lived happily ever after.
2. The dragon was never slain, but the princess lived happily until she didn't.
3. The dragon was slain at least twice.
4. The dragon was slain at most once.
5. Whenever the dragon was slain, the princess did not live happily.

*Answer:*

*Define*

*Define*

*Define =*

◻

1. ◻ ,
2. ,
3. ◻

**Proof**

Prove the following logical statements:

◻◻ ◻

◻

It may help to use these semantic definitions for ◻ and  (derivable from the definition in terms of ):

◻

You may use previously proven identities (both in this question and in lectures) to prove new ones.

Note that two temporal logic formulas  and  are logically equivalent, written , iff for all behaviours  it holds that:

*Answer:*

◻◻ ◻

Iff (by def)

Iff (by def)

Iff (by def)

Iff (by def)

◻

Iff (by def)

Iff (by def) ◻

 if and only if