CS5432 Homework 3: Information Flow

General Instructions. You may (but do not have to) collaborate with **one** other student on this assignment. If you do collaborate then both students should form a CMS group and submit their solution to that group. Both students are responsible for all of the answers.

Due: April 30, 2021 at 11:59pm. No late assignments will be accepted.

Submit your solution using CMS. Typeset your solution to produce .pdf, as follows:

- Use 10 point or larger font.
- Start each problem on a separate page.

---

1. Using the type system developed in class, prove that the following program satisfies Relational Non-Interference (RNI). Use the label assignment $\Gamma = \{x : L, y : H, z : H\}$ and an initial context $ctx = L$.

```
x := 42;
if y > 0
    then y := y – x
    else z := x + 1
fi
```

2. For each of the following programs and label assignments, determine whether or not the program satisfies (1) Termination Sensitive Non-Interference (TSNI), (2) Termination non-sensitive (aka Relational Non-Interference (RNI)).

a. $\Gamma = \{j : L, k : H\}$

```
k := 10;
while k > 0 do
    j := j + 1;
end
```

b. $\Gamma = \{m : L, n : L, p : H, q : H\}$

```
if n + m != -1
    then m := 7
    else
        if p < 5
            then q := p + 3
            else n := 13
        fi
fi
```

c. $\Gamma = \{i : L, j : H, k : H\}$

```
i := i + 10;
if i < 100
    then skip
    else
        while j != 0 do
            k := k + j;
            j := j – 1
        end
fi
```

d. $\Gamma = \{r : H, x : H, w : L\}$

```
if r mod 2 = 0
    then w := 0
    else
        x := (r + 1) mod 2;
        w := x
fi
```

3. We are given a programming language and type system (like was discussed in class) where all type-safe programs satisfy termination insensitive non-interference for the usual lattice involving L (public) and H (secret).

    a. You have been asked to endorse or reject a proposal to add a new built-in function, HRAND( ) to the programming language. Each time HRAND is called, it will return a value that has security label H and that is a random number. Thus, the history of past values it has returned tells nothing about future values it will return.
    b. You have been asked to endorse or reject a proposal to add a new built-in function, LRAND( ) to the programming language. Each time LRAND is called, it will return a value that has security label L and that is a random number. Thus, the history of past values it has returned tells nothing about future values it will return.