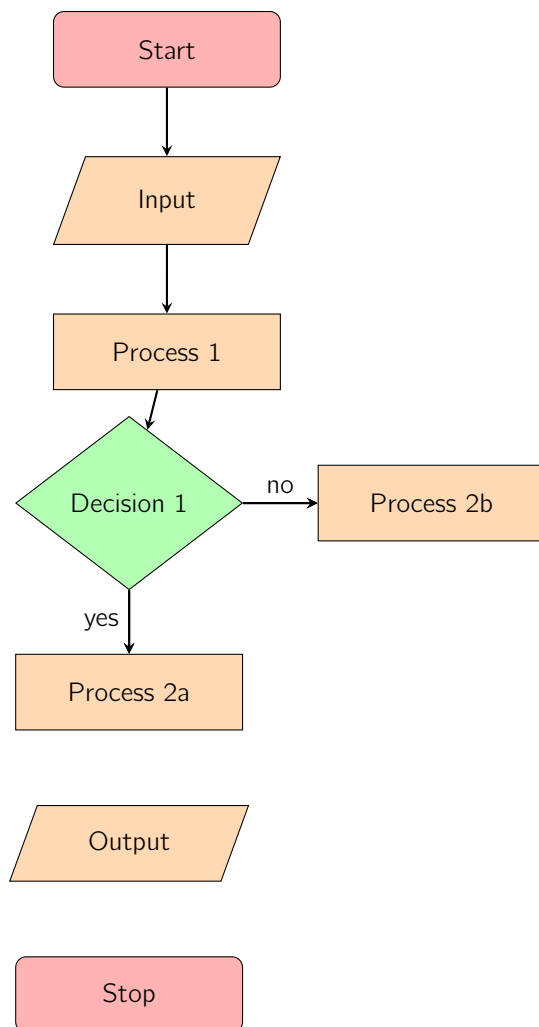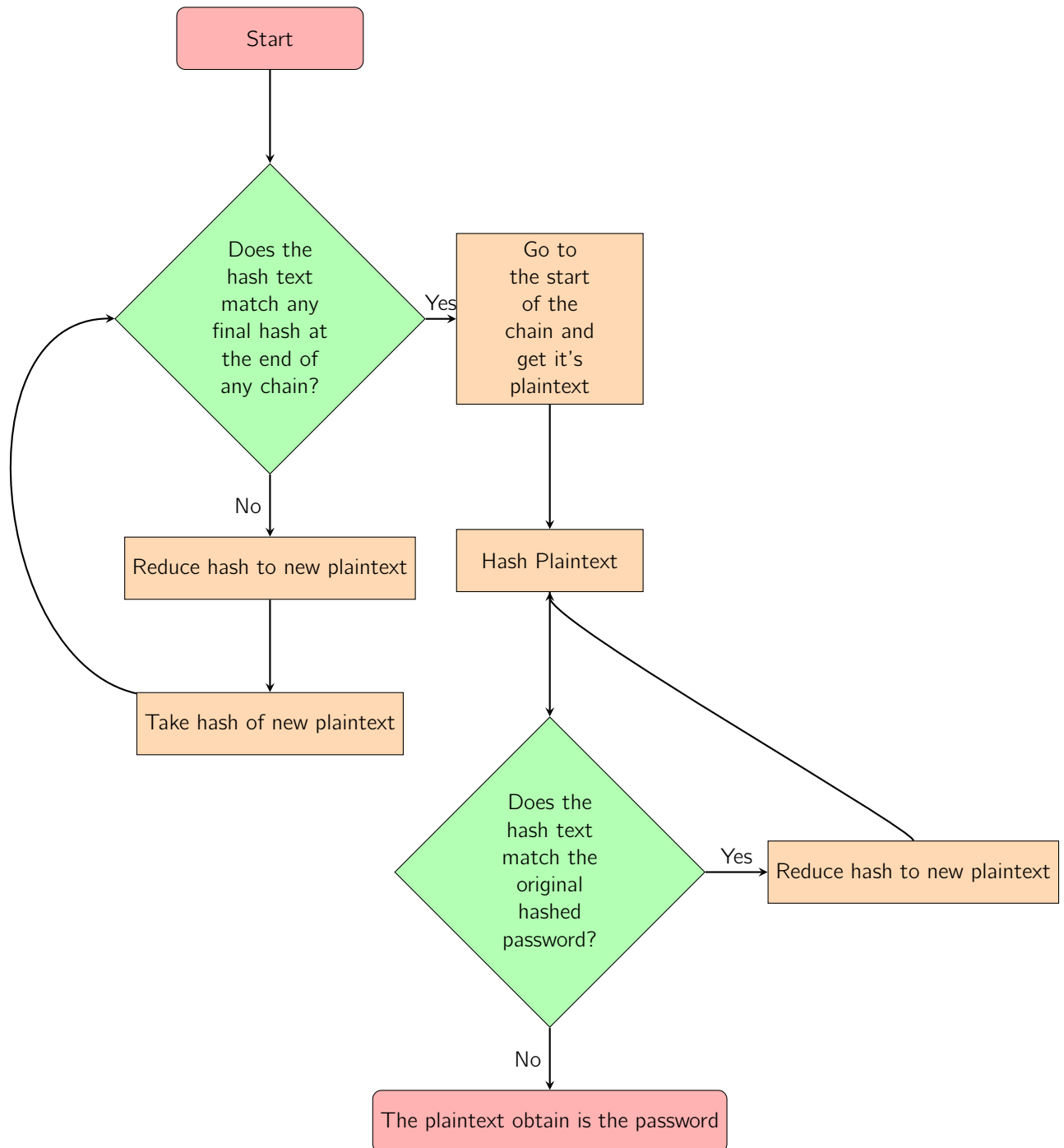# Lab-02: Describe Cryptographic Protocols with Diagrams and Flowcharts

Student Name     Avery Yong
Student #        059789115
Course Code      SPR200
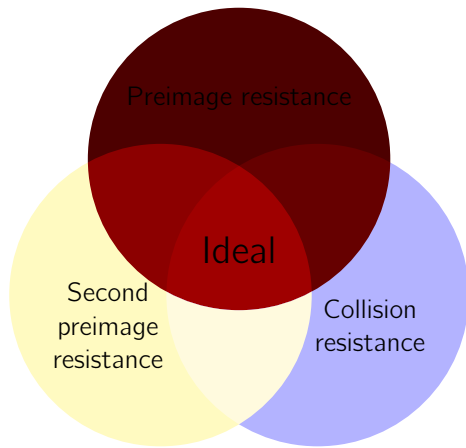Section Number   NAA
Professor        Prof. Wei Huang

## 1    Practicing Flowchart

# 2 Rainbow Attack Flowchart

```
                          ┌──────────┐
                          │  Start   │
                          └──────────┘
                                │
                                ▼
                        ╱╲                          ┌──────────────┐
                      ╱     ╲                        │   Go to      │
                    ╱  Does the ╲         Yes        │  the start   │
                  ╱   hash text   ╲─────────────────▶│   of the     │
                 ╱  match any final ╲                │  chain and   │
                 ╲  hash at the end ╱                │  get it's    │
                  ╲   of any chain? ╱                │  plaintext   │
                    ╲            ╱                   └──────────────┘
                      ╲        ╱                            │
                        ╲    ╱                              ▼
                          ╲╱                        ┌──────────────┐
                           │ No                     │Hash Plaintext│
                           ▼                        └──────────────┘
              ┌──────────────────────────┐                 │
              │Reduce hash to new plaintext│                ▼
              └──────────────────────────┘          ╱╲
                           │                       ╱    ╲
                           ▼                     ╱  Does the╲    Yes   ┌────────────────────────────┐
              ┌──────────────────────────┐     ╱  hash text  ╲───────▶│Reduce hash to new plaintext│
              │ Take hash of new plaintext│    ╲ match the    ╱        └────────────────────────────┘
              └──────────────────────────┘     ╲  original   ╱
                                                ╲hashed pass./
                                                  ╲  word?  ╱
                                                    ╲     ╱
                                                      ╲ ╱
                                                       │ No
                                                       ▼
                                        ┌───────────────────────────────┐
                                        │The plaintext obtain is the     │
                                        │         password               │
                                        └───────────────────────────────┘
```

# 3 Hash Function Properties Diagram

Preimage resistance

Ideal

Second preimage resistance

Collision resistance

# 4 Remote Coin-Flipping Protocol with One-Way Function

Sean Feng

GF

I don't understand this still