CSCI262 – System Security
Assignment 1

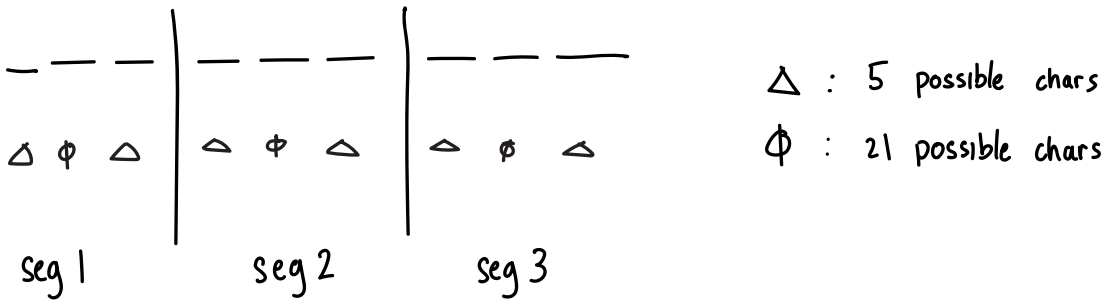
Timothy Mah
8750634
txamah001@mymail.sim.edu.sg

Part 1

Q1

A phonetic password generator picks two segments randomly for each six-letter password. Each segment has 3 English letters. The form of each segment is ΔΦΔ (consonant, vowel, consonant), where Φ is an element in {a, e, i, o, u} and Δ is an English letter which is not in {a, e, i, o, u}.
For example, "pampam" can be a possible output of the generator. However, "iamiam" is not.

How many possible passwords can the generator generate?



possible combi for 1 seg = 21 × 5 × 21
= 2205

possible combi for 1 pw (2 seg) = 2205 × 2205
= 4862025

The generator can generate 484205 possible passwords

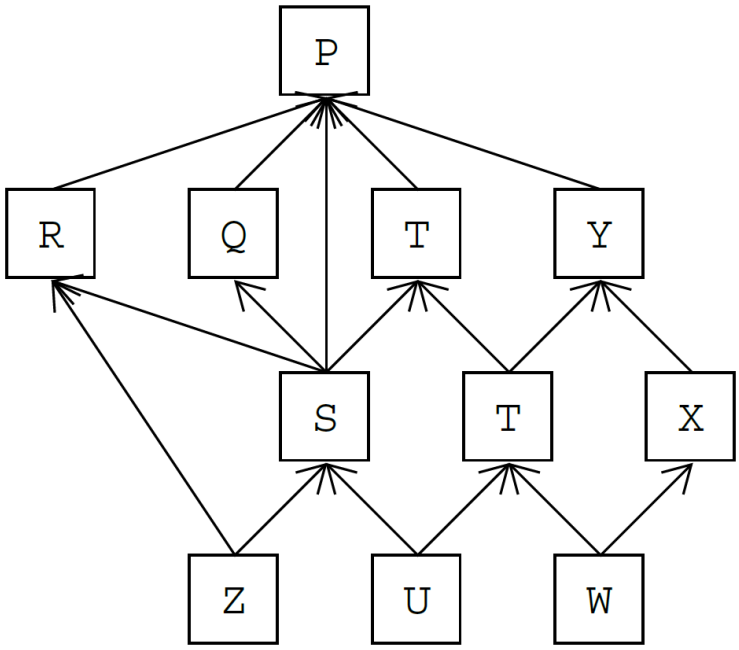
Q2

Assume that Alice has registered with the server Bob to use Lamport's one-time password scheme.
Alice's password is Alice1234567
If n = 5 initially, what are the first 3 one-time passwords transmitted by Alice? Use MD5 as the hash function.

Original pw = Alice1234567
n = 5
hash1 : 3e2a74a1ee147193d70e5266d7969468
hash2: 58d412d46635f99d5a65fc9b9d19b98f
hash3: f3ad0072adf2803a4dd7afd4ceec6d7d
hash4: 7620a7f4c73177c31620cdfe3eded58e
hash5: 121926a4319fcd814010090385c2e382
hash6: a4e4a69769bfcbca189b6a4b8599dc8d

otp1 = a4e4a69769bfcbca189b6a4b8599dc8d
otp2 = 121926a4319fcd814010090385c2e382
otp3 = 7620a7f4c73177c31620cdfe3eded58e

Q3



a. Does the diagram define a lattice? Justify your answer.

A lattice is a partially ordered set in which every pair of elements has both a least upper bound and a greatest lower bound
This diagram does not have a greatest lower bound hence it is not a BLP lattice

b. If the diagram does not define a lattice, assume you have corrected it so that it does, while maintaining the relationships between the existing levels. Some of the domination relationships in the diagram are redundant. Identify two such relationships and explain why they are unnecessary.

Z -> R and S -> P are unnecessary because there exists transitive relationships that describe them already

Q4

Consider the following statements and answer the subsequent questions:

Alexis can kick balls and throw sticks.
Boris can catch balls, kick balls, and throw sticks.
Catherine can snap sticks and roll balls.
Duggy the Dog can chew balls, fetch sticks and chew Boris.

a. What are the subjects, objects, and actions for this scenario?

Subjects: Alexis, Boris, Catherine, Duggy
Objects: balls, sticks, Boris
Actions: kick, throw, catch, snap, roll, chew, fetch

b. Draw an access control matrix representing this scenario.

subjects \ objects	balls	sticks	Boris
Alexis	K _ _ _ _ _ _ _	_ T _ _ _ _ _ _	
Boris	K _ C _ _ _ _ _	_ T _ _ _ _ _ _	
Catherine	_ _ _ _ _ R _ _	_ _ _ S _ _ _ _	
Duggy	_ _ _ _ _ _ C _	_ _ _ _ _ _ _ F	_ _ _ _ _ _ C _

c. Write a set of access control lists for this situation.

```
 “balls” : {“Alexis”:“K”}, {“Boris”:“K, Catch”}, {“Catherine”:“R”}, {”Duggy”:”Chew”}
“sticks” : {“Alexis”:“T”}, {“Boris”:“T”},        {“Catherine”:“S”}, {”Duggy”:”F”}
 “Boris” :                                                          {”Duggy”:”Chew”}
```

d. Write a set of capability lists for this situation.

```
 “kick” : {“balls”:“Alexis, Boris”}
“throw” : {“sticks”:“Alexis, Boris”}
“catch” : {“balls”:“Boris”}
 “snap” : {“sticks”:“Catherine”}
 “roll” : {“balls”:“Catherine”}
 “chew” : {“balls”:“Duggy”}, {“Boris”:“Duggy”}
“fetch” : {“sticks”:“Duggy”}, {“Boris”:“Duggy”}
```