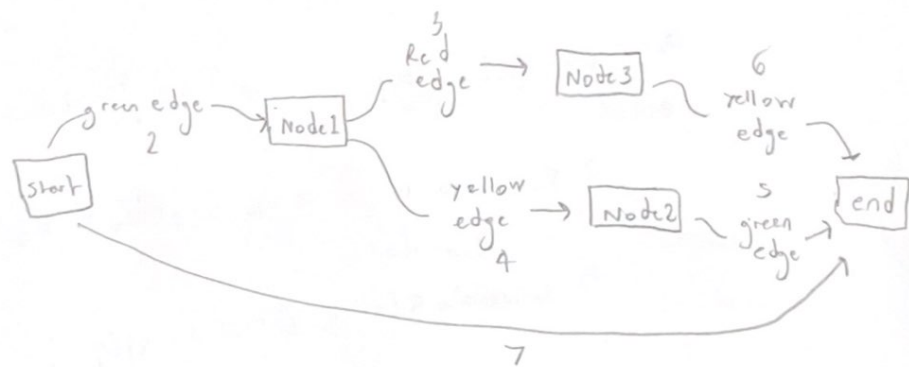


Mark Shinozaki

## 350 Homework 11



Problem 1: Enumerating the  $i$ -th Shortest paths from Initial to Final node

- Dijkstra's algorithm or A\* algorithm to find Shortest path
- Yes, after finding the Shortest path, Yen algo can be used to find the next  $k-1$  Shortest paths most efficiently

problem 2: Finding the Shortest path without a Red edge followed by a yellow edge

Problem 3

- DFS/BFS with state memorization
- Having color sequence
- counting unique sequences

→ Graph modification

- Remove any connection where red edge is directly followed by a yellow edge

→ Shortest path calculations

Problem 4.

- logarithmic time for nodes
- Shortest path algo

- Dijkstra's algo to compute the Shortest path from Initial to Final node

5. What is private key?

→ RSA public key where  $e = 49$ ,  $n = 10539750919$

→ Factorize  $n$  → Factorize  $n$  to find primes  $p$  and  $q$

→ Calculate  $\phi(n) \rightarrow \phi(n) = (p-1)(q-1)$

→ Calculate  $d \rightarrow d$  is such that  $(e \cdot d) \bmod \phi(n) = 1$

The prime factors of  $n = 10539750919$ ,  $p = 13481$   
 $q = 242399$

$$\phi(n) = (p-1)(q-1)$$

The private key exponent  $d$  is modular

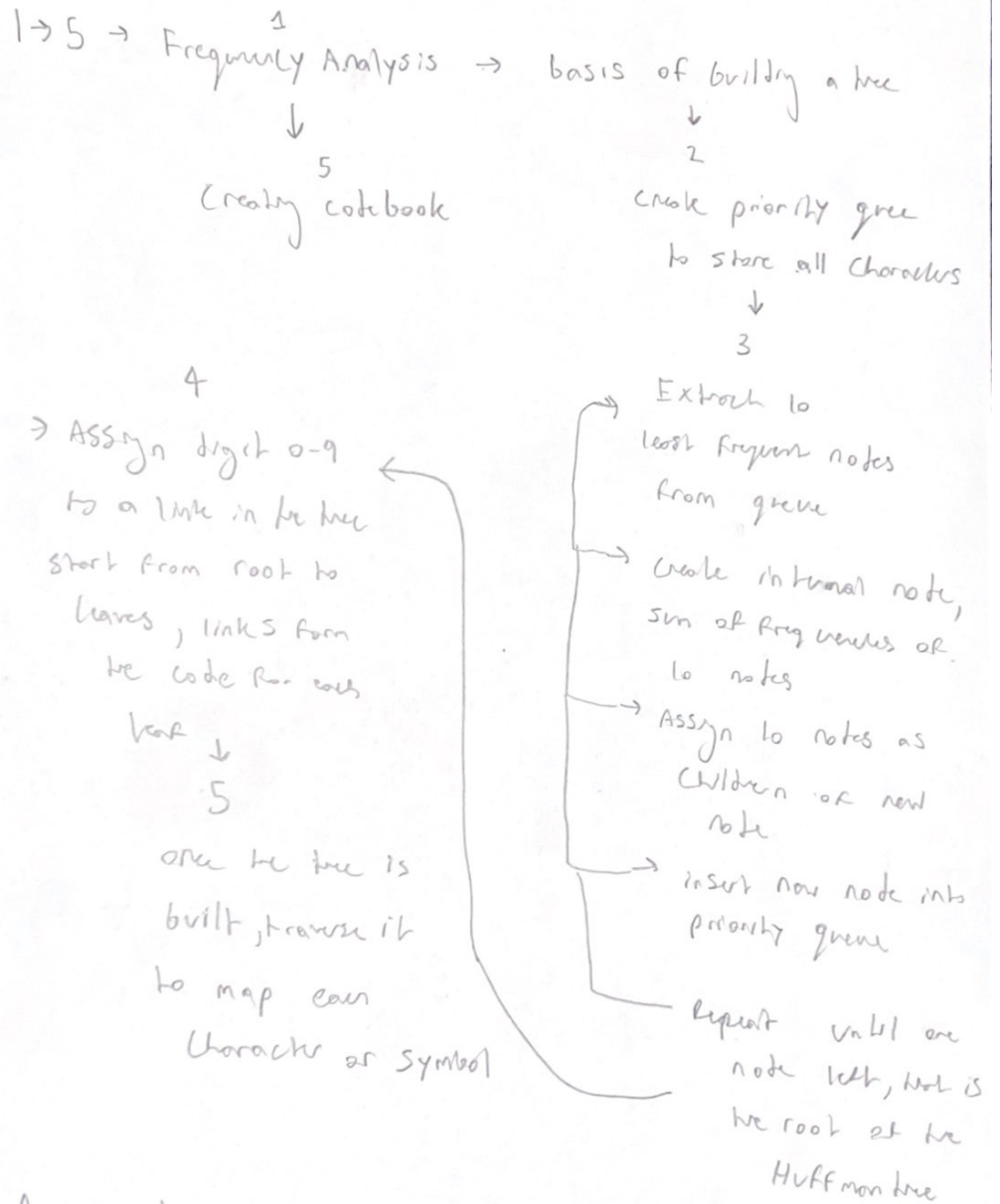
multiplicative inverse of  $e$  modulo  $\phi(n)$ .

The value of  $\phi(n)$  is 10,539,465,040, the

private key corresponding to the public key

$e = 49$   $n = 10539750919$  given by  $d = 3226366849$

6. Can you design a Huffman code algorithm?



7. Amortized analysis is a technique to assess the performance of an algorithm by averaging its resource consumption over a sequence of operations. This approach is useful because it considers both expensive and cheap operations, providing a balanced view over a worst case scenario. There are three methods to perform amortized analysis, aggregate accounting and potential methods