Assignment 2

Part 1

In this problem, we are going to have a simple hash function that can have a collision. We generate the hash function of an English word as follows:

Take the character - > Convert it to Binary Ascii - > 1 bit Right circular shift -> XoR with 101010101 -> Take the right most bit

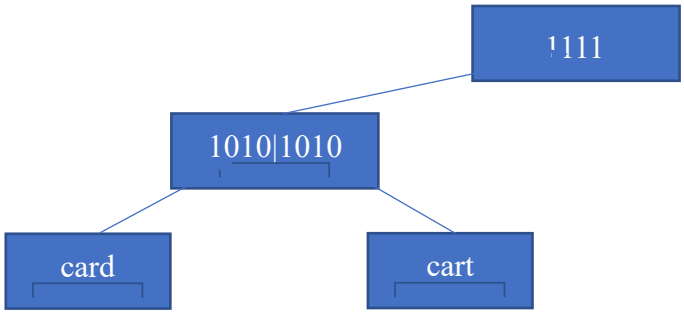
Find two different strings of length 4 that will produce the same hash value using the above hash function. You need to show the way you are computing the hash value. You will not get any point if you just write down the two strings.

“1989”
1 -> 49 -> 00110001 -> 10011000 -> 00110010 -> 0
9 -> 57 -> 00111001 -> 10011100 -> 00110110 -> 0
8 -> 56 -> 00111000 -> 00011100 -> 10110110 -> 0
9 -> 57 -> 00111001 -> 10011100 -> 00110110 -> 0

“EEEE”
E -> 69 -> 01000101 -> 10100010 -> 00001000 -> 0
E -> 69 -> 01000101 -> 10100010 -> 00001000 -> 0
E -> 69 -> 01000101 -> 10100010 -> 00001000 -> 0
E -> 69 -> 01000101 -> 10100010 -> 00001000 -> 0

Part 2

In your previous part, you constructed a hash value from a hash function. In this part, we are going to construct a Merkle tree from a list of word. In Markle tree structure, we pair words, computes the has values of each and then compute another hash value from the pair of hash values. Lets say, we have two words ‘card’ and ‘cart’ and we can construct the Markle tree as follows:



The construction is shown in the above diagram.

Using the above example as reference, construct a Merkle tree for the following words ,

dump, lamp, fact, hand, send, lock, mask, aunt

dump -> 0110 (Hash Value)
lamp -> 1010 (Hash Value)
fact -> 1001 (Hash Value)
hand -> 0101 (Hash Value)
send -> 1100 (Hash Value)
lock -> 0011 (Hash Value)
mask -> 1011 (Hash Value)
aunt -> 0100 (Hash Value)

Hash values of each pair:
dump|lamp -> 01101010 -> 11010101 -> 01111111 -> 1111
fact|hand -> 10010101 -> 01001010 -> 11110000 -> 0000
send|lock-> 11000011 -> 11100001 -> 01001011 -> 1011
mask|aunt -> 10110100 -> 01101101 -> 11000111 -> 0111

next level:
1111|0000 -> 11110000 -> 11111000 -> 01010010 -> 0010
1011|0111 -> 10110111 -> 01101111 -> 11000101 -> 0101

Finding final hash value:
0010|0101 -> 00100101 -> 10010010 -> 00111000 -> 1000

1000 is the root of the Merkle tree for the given words; dump, lamp, fact, hand, send, lock, mask, aunt .