MATH36206 Quiz6 Hash-based Signature Schemes

Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**INSTRUCTIONS:** Show all details in your solutions. Marks are given for the level of understanding shown. Good luck!

1. Find the Lamport public key and sign the message “0101” using with

**(2 marks)**

1. For a Merkle Tree with depth d = 3 with keys and hash function h(x) = x mod 17:
2. Determine the value of the root node. **(5 marks)**
3. Use the Merkle tree to sign the message . **(1 mark)**
4. Use the Merkle tree to sign the message . **(1 mark)**
5. How many messages can be signed using this Merkle tree? **(1 mark)**

