**Exercise 5**

**Student ID: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Student Name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**Short Answer Questions:**

1. Which criterion ensures that we cannot find a message that hash to the digest of a given message.

2. Which criterion ensures that we cannot find two messages that hash to the same digest.

3. Which criterion ensures that we cannot find a message that hash to the specified digest.

4. How is a hash function used to generate and verify digital signature?

5. What are the two phases of the sponge construction for SHA-3?

6. In SHA-3, which among Theta, Rho, Iota, Pi and Chi is permutation operation?

7. In Keccak-f [1600], if the capacity = 512, what is the bitrate ‘r’?

8. In Keccak-f [1600], if the capacity = 256, what is the security level?

9. How many iterations / rounds does the Keccak-f[1600] function have?

10. By the Pi operation of SHA-3, which lane is the lane A[2, 1] of a state permuted to?

11. Keccak Hash Function (SHA-3) uses the sponge construction.

(a) Please explain the two phases of a Sponge hash function to generate a hash value of a given input.

(b) What are the purposes of the two variables r and c, respectively?

12. In Keccak-f, the state can be considered to be a 5 × 5 × 2l array of bits and *χ* is a nonlinear mapping as shown in the following figure.

Assume that one row of the state is 01011, determine the row of the state after *χ* operation.