

## **Part 1**

- (a). message digest was created and saved in the folder hash.
- (b). Done and stored in folder encryption.
- (c). From ECB we can derive some information about the original picture like the shape in the picture the colour etc. From CBC we can not derive any information.
- (d). The hashes were created and stored in the folder hash. No they are very different and count gives value 0 for the specific hashes.

## **Part 2**

### **Task1**

- 1. 20000000 trails and still sometimes bad luck.
- 2. 20000 trails.
- 3. Collision property is easier to break.

### **Task2**

The answer is Median

## **Part 4**

The answer is 'thedancingmen'