**Q1**

Chosen Password: wD05@Ag9$J

|  |  |
| --- | --- |
|  | possibilities |
| 1. Lower case letter (a-z) | 26 |
| 1. Upper case letter (A-Z) | 26 |
| 1. Digit (0-9) | 10 |
| 1. Digit (0-9) | 10 |
| 1. @ | 1 |
| 1. Upper/Lower case letter (a-z, A-Z) | 52 |
| 1. Upper/Lower case letter (a-z, A-Z) | 52 |
| 1. Symbol {$,9,5,v,w,J} | 6 |
| 1. Symbol {$,9,5,v,w,J} | 6 |
| 1. Symbol {$,9,5,v,w,J} | 6 |

Entropy = L log2N

N = 26 x 26 x 10 x 10 x 1 x 52 x 52 x 6 x 6 x 6

= 39,482,726,400 or 3.95 x 1010

Entropy = 1 log2 (39,482,726,400)

≈ 35.20 bits

Entropy of Tiger Hash = 10 log2Tiger 3.95 x 1010

Tiger(wD05@Ag9$J) = 357c723ff871393085c9e40f401679187fad4f78f3959d52

**Q2**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | O1 | O2 | O3 | O4 | O5 | O6 |
| S1 | R | R | R | R | R | RW |
| S2 | R |  |  | W | W | W |
| S3 | R | RW | RW |  | W | W |
| S4 | R |  |  | R |  | W |
| S5 | R |  |  |  |  |  |
| S6 | R | R | R |  | R |  |

|  |
| --- |
|  |

Subjects from every level can read object O1 and is dominated by all subject, hence it is at the lowest level

|  |
| --- |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | O1 | O2 | O3 | O4 | O5 | O6 |
| S1 | R | R | R | R | R | RW |
| S2 | R |  |  | W | W | W |
| S3 | R | RW | RW |  | W | W |
| S4 | R |  |  | R |  | W |
| S5 | R |  |  |  |  |  |
| S6 | R | R | R |  | R |  |

Subject S3 can read and write objects O2 and O3, hence S3, O2, O3 must be at the same level.

|  |
| --- |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | O1 | O2 | O3 | O4 | O5 | O6 |
| S1 | R | R | R | R | R | RW |
| S2 | R |  |  | W | W | W |
| S3 | R | RW | RW |  | W | W |
| S4 | R |  |  | R |  | W |
| S5 | R |  |  |  |  |  |
| S6 | R | R | R |  | R |  |

|  |
| --- |
|  |

Subject S5 can only read object O1, hence subject S5 can only dominate object O1.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | O1 | O2 | O3 | O4 | O5 | O6 |
| S1 | R | R | R | R | R | RW |
| S2 | R |  |  | W | W | W |
| S3 | R | RW | RW |  | W | W |
| S4 | R |  |  | R |  | W |
| S5 | R |  |  |  |  |  |
| S6 | R | R | R |  | R |  |

|  |
| --- |
|  |

Subjects S1 and S6 must dominate Object O2 and O3 to allow reading

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | O1 | O2 | O3 | O4 | O5 | O6 |
| S1 | R | R | R | R | R | RW |
| S2 | R |  |  | W | W | W |
| S3 | R | RW | RW |  | W | W |
| S4 | R |  |  | R |  | W |
| S5 | R |  |  |  |  |  |
| S6 | R | R | R |  | R |  |

Subject S1 and S4 must dominate object O4 to allow reading.

|  |
| --- |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | O1 | O2 | O3 | O4 | O5 | O6 |
| S1 | R | R | R | R | R | RW |
| S2 | R |  |  | W | W | W |
| S3 | R | RW | RW |  | W | W |
| S4 | R |  |  | R |  | W |
| S5 | R |  |  |  |  |  |
| S6 | R | R | R |  | R |  |

Subject S1 must dominate object O5 to allow reading.

O5 must dominate Subject S2 and S3 to allow writing.

|  |
| --- |
|  |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | O1 | O2 | O3 | O4 | O5 | O6 |
| S1 | R | R | R | R | R | RW |
| S2 | R |  |  | W | W | W |
| S3 | R | RW | RW |  | W | W |
| S4 | R |  |  | R |  | W |
| S5 | R |  |  |  |  |  |
| S6 | R | R | R |  | R |  |

O6 must dominate S4 to allow writing.

Top level introduced to complete the lattice.

**Q3**

|  |  |  |  |
| --- | --- | --- | --- |
| **Statement** | **Subject** | **Objects** | **Actions** |
| Alice can climb trees and eat apples | Alice | Trees and Apples | Climb, Eat |
| Bob can climb fences, eat apples, and wave flags | Bob | Fences, Apples, Flags | Climb, Eat, Wave |
| Trees can hurt apples. | Trees | Apples | Hurt |
| Carol can jump waves and wave flags | Carol | Waves, Flags | Jump, Wave |

Legends: Climb = C , Eat = E, Wave = W, Hurt = H, Jump = J

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Subject/Objects** | **Apples** | **Fences** | **Flags** | **Trees** | **Waves** |
| **Alice** | E |  |  | C |  |
| **Bob** | E | C | W |  |  |
| **Trees** | H |  |  |  |  |
| **Carol** |  |  | W |  | J |