
Extra Credit #2

Due: May 7, 2021

Points: 30

Questions

1. (15 points) Prove Theorem 6.1 for the strict integrity policy of Biba's model.
2. (15 points) The index of coincidence was defined as "the probability that two randomly chosen letters from the ciphertext will be the same." Derive the formula in Section 10.2.2.1 for the index of coincidence from this definition.