Homework 3

Task 1 - Key Recovery (5 + 5 points)

(a)

(b)

Task 2 - When IVs Collide (8 points)

(a)

(b)

Task 3 - IND-CPA Security (10 points)

(a)

(b)

Task 4 - Padding-Oracle Attack (22 points)

(a)

(b)

(c)