Problem Sheet 5

Problem 5.1
Solution:

b)
./src/main -k 0x98267351 secret

b: ecb
k: 0x98267351
m: 0x736563726574 ″secret″
c: 0xd3b0d2c3b0a1
d: 0x736563726574 ″secret″

c)
./src/main -k 0x98267351 -i 0x42 hacker

b: cbc
k: 0x98267351
i: 0x42 ″B″
m: 0x6861636b6572 ″hacker″
c: 0x66b6bbe90e21
d: 0x6861636b6572 ″hacker″

d)
bob loves alice