Homework 3

1) D

2) C

3) Key = $K = 0^l$ $Enc_K(m) = K \oplus m = m$

Key $K \neq 0^l$

$K = 1^l$

$m_1 = 0$ $C = 0$ output 0

$m_2 = 1$ else $C = 1$ output 1 $K = 1$

$[Pr\ A \text{ outputs } 1 \text{ in } Exp_0] = [Pr\ A \text{ outputs } 1 \text{ in } Exp_1]$

$= 1$ $= 0$

not perfectly indistinguishable

not perfectly indistinguishable

When generating keys they had to be shared

implimentations

NOT AN IMPROVEMENT

By looking at the cipher text the adviserary could still try to decrypt the message, however since we are using OTP there can always be two possible ways that the message was encrypted, you can encrypt the message with the same key as the message.

Homework 3

5)

a) False using symmetric encryption the two parties must first share a key Secretly. The provide Confidentiality, a secret key must first be shared.

b) True With a message space of one character, it would fit the definition of perfectly indistinguishable.

c) True OTP is considered indistinguishable even with a infinite computational power and time it can't be broken.

d) False a encryption is not indistinguishable with a longer key.

e) False Gsm encryption can be cracked