Homework 1

January 2019

1 Exercise 3

1.1

Plaintexts and cyphertexts are of size n.

1.2

Given a pair (m, c), the brute force attack consists in searching the $2^l \times 2^l$ key space for the pair of keys (k_1, k_2) such that $Enc_{k_1,k_2}(m) = c$.

1.3

Given a pair (m, c), an attack can use the $n2^l$ memory space in the following way:

- For each key k_1 in the 2^l key space, encrypt the plaintext m and store $Enc_{k_1}(m)$ along with the key k_1 in memory.
- For each key k_2 in the 2^l key space, decrypt the cyphertext c using $Dec_{k_2}(c)$ and look for a match in the memory space.
- If a match is found, return the corresponding k_1 and k_2.

1.4

Given a pair (m, c), an attack can use the $n2^l$ memory space in the following way:

- For half of the keys k_1 in the 2^l key space, encrypt the plaintext m and store $Enc_{k_1}(m)$ along with the key k_1 in memory.
- For half of the keys k_3 in the 2^l key space, decrypt the cyphertext c and store $Dec_{k_3}(c)$ along with the key k_3 in memory.
- For each key k_2 in the 2^l key space, decrypt the cyphertext c using $Dec_{k_2}(c)$ and look for a match in the memory space.
- If a match is found, return the corresponding k_1 and k_2.