Secure and Dependable Systems – Homework #6

Sagar Kumar

Problem 6.3:

Part a)

The first thing to note is that the substitution is a simply function that maps a “”finite” to set another “finite” set. Meaning that the time to assess the set is finite and for small sets brute force searches are sufficient. Hence def 15.18 holds. However the probability of finding the correct solution is where p(x) is the negligible function. For the next step the proof will follow like shown previously because the finite set is the same. I.e. the probability will also be the same . For the third step each bit can either be 0 or 1. The probability then becomes . Even though a brute force search will take a significant amount of time, the solution can still (theoretically) be found. Using IV: we now observe that changing the keys does not make a difference as the result is still 0 or 1. Because each step are negligible, the entire process becomes negligible

Part b)

For this system, it is easily possible to decrypt through reverse engineering, namely by giving it a random input string. Consider the example 15.20: We consider a few outputs from the system and hence generate the key accordingly. For each bit we can use XOR for each encryption step and also for decryption. Thus, the encryption is not safe against CPA (chosen plaintext attack).