**CS6014 Crypto Homework**

**U1426365 Jin-Ching Jeng**

## Question 1 (5 points)

A block cypher with an 8 bit block size is very easy to break with a known-plaintext attack (assuming each block is just encrypted independently with the same key). Describe how you would do so.

Because the number of possible permutations is 2^8 = 256, it is not too hard to resolve the table between plaintext and cyphertext. If they use the same rule to encrypt other messages next time, it’s easy to break it by comparing the table.

## Question 2 (10 points)

Assume you're sending a long message using a block cypher (like AES) with the following scheme: split the message into blocksize chunks, then encrypt each with the same key. Basically Alice sends Bob AES(m1, k), AES(m2, k), AES(m3, k), etc.

* a(3 points): Even if they can't decrypt blocks, what information can an eavesdropper discern from this scheme? Hint: imagine Alice is sending a table of data where each cell is exactly one block of data.

The eavesdropper can know the length of the message by knowing how many blocks there are. Also, if there are two same ciphertexts, their plaintexts are the same.

* b(4 points): Things are actually even worse! A malicious attacker can actually CHANGE the message that Bob receives from Alice (slightly). How? This is particularly bad if the attacker knows the structure of the data being sent (like in part a)

If the attackers know the structure of the data (like each cell is one block of data), they can change the message by changing the order of the blocks. In this way, the decrypted message of each block is the same but in a different order from the original.

* c(3 points): How could you modify the scheme to mitigate/prevent these types of attack?

Alice can put some information about the order of the message in each encrypted cyphertext.