Assignment 1
Burhanuddin Mogul
CS 408 001 Cryptography & Internet Security

Problem 1

a) Without knowing the key, the ciphertext “EVIRE” can be decoded to both “RIVER” with a key of 13, meaning a shift of 13 letters in the alphabet, or it can be decoded to “ARENA” with a key of 22, meaning a shift of 22 letters in the alphabet.
b) Ceaser can send another message with the same key as he initially intended, but before sending it he should verify that the message cannot be decoded with the other key. If the key was meant to be 22, then send the ciphertext “pda gau sehh iwpyd pdeo iaoowca” which will decrypt to “The key will match this message” if 22 is used but if 13 is used it will be gibberish.
c) Involutory for Z_{26}, Z_{22}, and Z_{23} in a Shift cipher are keys where $E_k(P) = D_k(P)$. 0 is a given as it does not do any shift
    a) Z_{26} = 0, 13
        a) A – 13 and A + 13 both give a value of N, in the alphabet of 26 letters
    b) Z_{22} = 0, 11
        a) In an alphabet of 22 letters, shifting 11 forward or 11 backward will give the same value
    c) Z_{23} = 0
        a) No key other than 0 will yield the same E_K and D_k

Problem 2

a) As the plaintext is one repeated letter, after every 6 letters, Eve would notice that the pattern repeats for the entire ciphertext.
b) Eve would be able to determine the key by using the distance between each letter in the ciphertext, as they represent the distance between each letter of the key. Once each distance is determined, Eve now has constraints for the key (the distance between the letters of the key) and would need to try each possibility until the key breaks the ciphertext. Eve would then have to try the 26 different options for the key (generated by the constraints of the key found earlier) and only one would be a valid English word. The key would be unique as the positions of the letters in the key are fixed and there are only 26 possible options. We know that no English word of length 6 is a shift of another, therefore we would not find any other English words that would match this constraint.

Problem 3

a) The first step of the DES algorithm is the initial permutation, which is based off of a vertex that reorders the bits. So if we were to take the compliment of *x* and then perform IP or if we were to perform IP and then take the compliment we would get the same value, or

$$IP(\overline{x}) = \overline{IP(x)}$$

Now we know that the result of IP is not affected by bitwise compliment. Next we can look at the expansion function, the expansion function is XOR with the key k.

$$E(\overline{x}) \oplus \overline{k} = \overline{E(x)} \oplus \overline{k} = \overline{E(x) \oplus k} = E(X) \oplus k$$

We can see that the input to the S-Boxes is the same regardless of bitwise complementation. The final permutation will follow the same logic. Therefore, the end result means that the compliment of $Y = DES_k(x)$

b) An attacker can reduce the expected number of keys to be tried in a brute force chosen-plaintext attack by half by using the complementation property of DES assuming they have a pair of plaintext and ciphertext as follows; (M_1, C_1) and ($\overline{M_1}$, C_2). The attacker can initially try all keys that start with 0, this eliminates half the keys. Assuming this does not work, the attacker can try the same set of keys but on the compliment of M_1. By doing this the attacker would eventually get the compliment of C_1 and once they do they have found the compliment of the key.

Problem 4

a) Semi weak keys are keys such that K_1 and K_2 are not equal and $E_{K1}(E_{K2}(P))$ for some plain text will yield P if the keys are *semi weak*. This would mean that the round keys they generate are the same but in inverse order. As what is happening is that the Ciphertext generated by K_2 is being decrypted by K_1, and we know decryption in DES is the same as Encryption but using the round keys in reverse order.

b) The danger of using a pair of *semi weak* keys is that they decrypt each other. If one was to perform DES twice with *semi weak* keys, it would simply decrypt the original encryption, if they were to do triple DES it would be the same as doing single DES assuming the encryption uses the same pair of *semi weak* keys.