Note from the professor:

“Let me add more description to the second question of the homework assignment.

First of all, the 128 bit key I provided needs to be used for key whitening.

So, you don't have to run the key addition layer in the first round.

After the key whitening, your intermediate state (the result from the key whitening) should go through the byte substitution layer and the diffusion layer.

For the MixColumn transformation, just get the first four byte results which are C0, C1, C2, and C3.

Hope this would minimize tedious work”.

1. (35 pts) for the given plaintext, what would be the state (intermediate cipher) after the first round of DES?

PLAINTEX

(01010000 01001100 01000001 01001001 01001110 01010100 01000101 01011000)

48 bit key

(11010111 00001010 01011101 00100010 10000011 11010101)

2. (35 pts) For the given plaintext, what would be the state (intermediate cipher) after the first round of AES?

CIPHERTEXT BLOCK

(01000011 01001001 01010000 01001000 01000101 01010010 01010100 01000101 01011000 01010100 01111111 01000010 01001100 01001111 01000011 01001011)

128 bit key

(10100010 11000111 10101110 11110101 11000010 10010111 01000100 01010100 00001111 01010101 00010100 10111010 00100010 10100000 01111010 10101001)

3. (10 pts) Assume a group of 20 people would like to have pair-wise secure communications. How many keys need to be exchanged in total?

**For Symmetric System: -**

Each time a new user is added to the system, it needs to share a new key with each previous user. Thus, for n users, we have 1 + 2 + . . . + ( n − 1) = n ( n − 1) /2 keys.

= 20\*19/2

**= 190 keys**

**For Asymmetric System: -**

Each time a new user is added to the system, it needs only a public key and a private key. Thus, for n users, we have 2 n keys

So total number of keys would be 2 \* 20 = 40 keys.