1. Stream Cipher works using the xor operation. Assume the first ten bits of plaintext are 1101010010… the key starts with 0001110101… What is the cipher text after encryption?

After encryption the cipher text would be 01010101 00000110 01010000 11010100

1. For DES encryption, assuming the input plaintext is:

01011010 01011010 01011010 01011010 01011010 01011010 01011010 01011010

What is the output of the Initial Permutation (IP)?List the last 5 bits. The mapping table is shown as below: (10 points)

11111111 11111111 00000000 00000000 00000000 00000000 11111111 11111111

1. DES has 56-bits key. How many hours will it take a brute force attacker to test all keys, assume the attacker can decrypt with 10^12 times per second. Show your calculations.

Now we want to find the number of decryptions in base 2

So this means we our attacker can decrypt keys per second (kps)

To determine how many hours this would take we can now take the number of possible keys and divide this by the number of potential keys per hour, pluggin in values from above we find that

1. This question has 2 parts
   1. If the 3rd byte is in error, and we know that in CBC all blocks are dependent on the previous this would mean the first block is corrupted which in turn corrupts the blocks after it so each subsequent block including the 1st block would be corrupted
   2. If the 3rd byte and 18th byte are in error we have an error in the 1st and 2nd blocks, this should follow the same principle as the question above, thereby meaning every block should also be effected
   3. Answer is the same for this segment as well, Block 1 and Block 3 are in error and therefore we have errors in all the blocks
2. Confidentiality would be achieved, the use of the public and private keys would ensure that only Alice would be able to open and read the message
3. I would choose the CBC method of cryptography, because the candidate names are fixed, I have a limited set of plaintexts that I need to choose from. With a properly unpredictable IV this method would be safe from chosen-ciphertext attacks
4. This question has two parts
   1. This scheme can protect against transmission error, as flipping a couple of the bits would invalidate the hash making the message unreadable, so Bob could know that the message had not been transmitted successfully, it would potentially be difficult for Bob to know where the switch took place
   2. This scheme can protect against an interception and injection the hash is specific to that message and simply injecting in to the hash would not be sufficient to generate a new message and the message cannot be derived from the hash alone