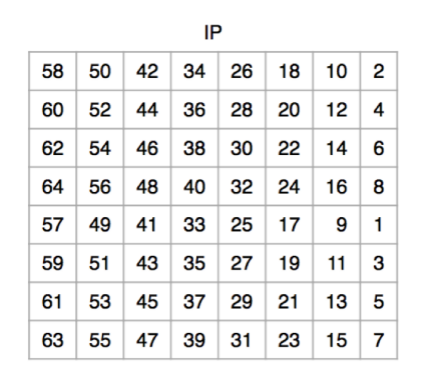
Homework 2

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? (10 points)
2. 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)



1. DES has 56-bits key. How many hours will it take for the brute-force attacker to test all keys? Assume the attacker could decrypt with 10^12 times per second. Show your calculation. (10 points)
2. In the CBC mode of AES-128 algorithm, each block is in 16 bytes length.
3. If byte 3 in ciphertext is in error, what block/blocks will be in error after decryption? (7 points)
4. If byte 3 and byte 18 in ciphertext are both in error, what block/blocks will be in error after decryption? (7 points)
5. If byte 3 and byte 39 in ciphertext are both in error, what block/blocks will be in error after decryption? (6 points)
6. Bob is trying to send a secure message to Alice.

By generating these ciphertexts: C1 = Epub\_A(P), C2 = Epriv\_B(C1), what security property could be achieved? (10 points)

1. If you want to securely send a vote result to the voting center. Two candidates’ names are John and Kathy, what encryption mode should you choose from these: ECB, CBC, CFB, OFB. And why? (10 points)
2. Consider the scheme: Alice sends a message M to Bob. To make Bob to verify the content is authentic, Alice made a hash over the message M, i.e., to generate hash(M), and send (M,hash(M)) together to Bob. Assume the message is not encrypted by any other means.
3. Could this scheme protect against transmitting error? (E.g., if a transmitting error happens by flipping a bit or two due to bad link quality, could Bob discover it?) (10 points)
4. Could this scheme protect against an malicious attacker that can intercept and inject into the transmission? Why? (10 points)