Homework 2

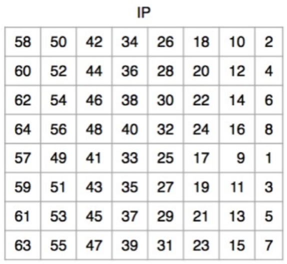
1. Stream cipher works using the xor operation. Assume the first ten bits of plaintext are 1101010010.... The key starts with 0001110101.... What is the cipher text after encryption? (10 points)

1100100111

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)



IP

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

11111

3. 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)

(2^56/10^12) / (60 * 60) = 20.02 hrs

4. In the CBC mode of AES-128 algorithm, each block is in 16 bytes length.

1) If byte 3 in ciphertext is in error, what block/blocks will be in error after decryption? (7 points)

All of block 1 will be corrupted.

-4

2) If byte 3 and byte 18 in ciphertext are both in error, what block/blocks will be in error after decryption? (7 points)

-4

All of block 1 and block 2 will be corrupted.

3) If byte 3 and byte 39 in ciphertext are both in error, what block/blocks will be in error after decryption? (6 points)

All of block 1 and block 3 will be corrupted. -3

5. 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)

Confidentiality and Authenticity is achieved.

6. 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)

CBC cause as long as the IV is not predictable or stored/transmitted in plaintext it has more steps in the encryption and also it is not vulnerable to pattern or cryptic analysis.
ECB: same plaintext *m*,  same ciphertext *c*
Also CBC: same plaintext *m*, different ciphertext *c*

-4

7. 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.

1) 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)

encryption is meant to protect data in transit, hashing is meant to verify that a file or piece of data hasn't been altered, that it is authentic. In other words, it serves as a check-sum.
hence bob can find out if any transmission error occurs while message transfer.

2) Could this scheme protect against an malicious attacker that can intercept and inject into the transmission? Why? (10 points)

The integrity check helps the user to detect any changes made to the original file. It, however, does not provide any assurance about originality. The attacker, instead of modifying file data, can change the entire file and compute an all-together new hash and send it to the receiver. This integrity check application is useful only if the user is sure about the originality of the file. Man-in the middle attack will be one of them where an attacker can send his own message impersonating Bob. Also, depending on your type of hash function, some hash functions can be easily attacked two files with the same hash value making it very unsecure and prone to attacks. A good example to that would be md5 which is less secure as compared to sha256.