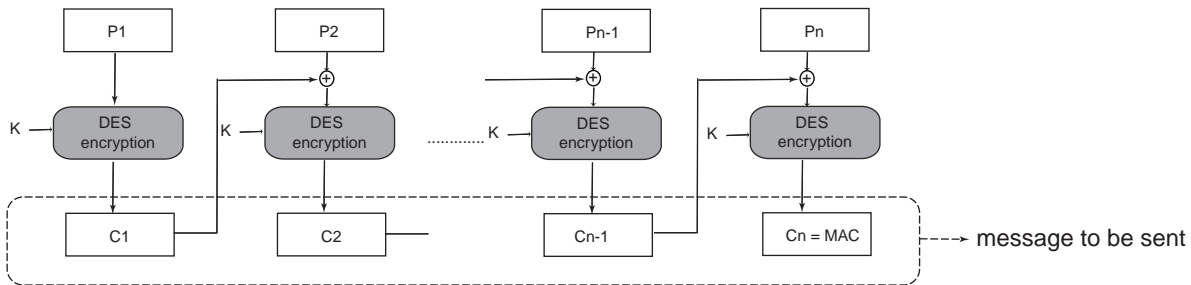


Homework 2

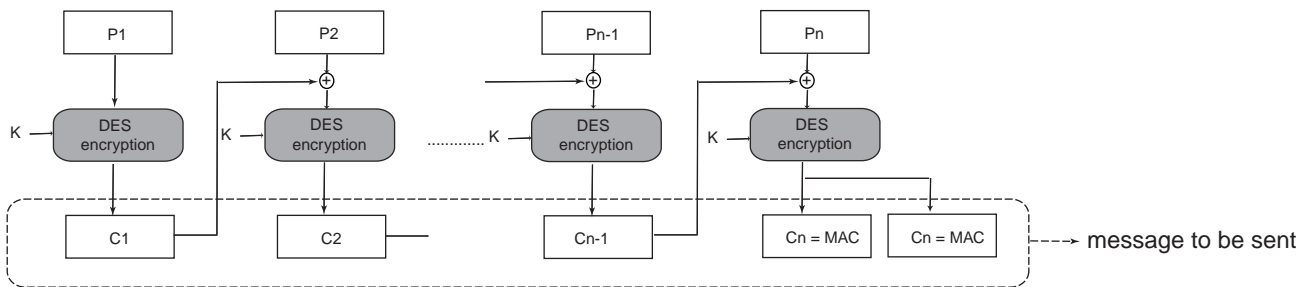
Due date: October 7

1. (20 pts) With symmetric ciphers, you are ready to communicate with your friends in a secure way. First let's consider the problem of communicating with one of your friends Bob.
 - Assume that you and Bob share a secret K (*i.e.*, shared master key). Could you describe the procedure how the two of you acquire the key (session key) for communication? (10 pts)
 - Using this session key, you first wish to send Bob an email. At which layer of the network stack are you going to use the encryption scheme, and why? If you and Bob transfer files in a peer-to-peer fashion, at which layer should the encryption be used? (10 pts)
2. (35 pts) Now let's consider the problem of communicating among your friends: Alice, Bob, Cathy, Doug and yourself. Consider the following communication scenarios:
 - (a) The only communication in your group is broadcast (*e.g.*, a message or a file is sent from you, and received by all other group members). The content of the communication needs to be protected from the interception of any other person outside your group.
 - (b) Communication between any two group members are possible, and needs to be protected from anyone else.
 - Without a key distribution center (KDC), please discuss the minimum number of master keys required in each of the above scenarios. What if there is a key distribution center? (5 pts)
 - Could you describe the procedures to acquire the session key in each of the above scenarios (group communication and communication between two members; with and without a key distribution center)? (10 pts)
 - Now you wish to send an email to all members of your group using the session key you just got. Please describe the procedure. What if you want to send a file to all of them? (5 pts)
 - With shared session key(s) among your group members, your previous designs are confined to an end-to-end encryption approach. Now let's consider an alternative approach where routers/switches provide encryption supports. Please describe the procedure to send an email to all your group members. (Reference: Problem 7.1 in textbook [WS]) (5 pts)
 - In the first scenario, your group wish to provide data source authentication (assuring who broadcasts in the group) in addition to the data confidentiality. Please discuss whether it can be achieved via the symmetric key encryption. If so, how? If not, why? How about the second scenario (*i.e.*, assurance of the data source in the communication between two group members)? (10 pts)

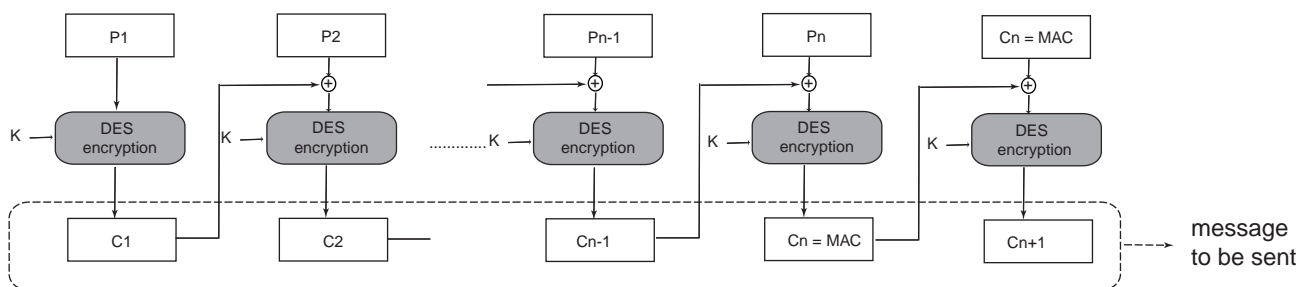
3. (15 pts) As we know, Message Authentication Code (MAC) can be generated using CBC mode of operation of DES. Alice claims that she can send C , the encrypted message of plaintext $P = (P_1, P_2, \dots, P_n)$ via DES in CBC mode, as shown in Fig. 3(a), to achieve the goal of both data confidentiality and integrity, because MAC is included in the message to be sent. Bob claims that Alice's scheme can only achieve data confidentiality, but not data integrity. To achieve data integrity, additional MAC needs to be appended to C , as shown in Fig. 3(b). On the other hand, Cathy claims that the MAC needs to be appended to the plaintext instead of ciphertext for integrity protection. And for confidentiality, the plaintext with its MAC needs to be encrypted as shown in Fig. 3(c). Please identify the valid claim. If there is none, please present a way to achieve both data confidentiality and integrity only using DES algorithm and CBC mode of operation.



(a) Alice's scheme



(b) Bob's scheme



(c) Cathy's scheme