Assignment 2
Gunnar Yonker

1. Double DES is the process of applying the DES encryption algorithm process twice to the same set of data that is being encrypted. This does not actually make the encryption stronger because it still allows the double encryption to be attacked by using a sort of “meet in the middle” attack. This allows an equation to be used when a cipher is used twice(C=EK2(EK1(P))). Then the equation X = EK1(P) = DK2(C) is used. The attack is carried out by encrypting P with all keys and then decrypting C with all keys with the goal of matching the X values. If they match they will produce the correct ciphertext and can be accepted as the correct keys to then be used to attack and break the Double DES encryption. The amount of work it takes to complete this process is less than that of a brute force attack on the double DES encryption so it is not any more secure than a single round of DES encryption. For stronger encryption than DES, AES and Triple DES is used.

2.

(1) CTR is the only of the three modes that allows for parallel encryption and decryption. CFB and OFB allow for parallel decryption but not parallel decryption.

(2) For counter operation mode(CTR) you never want to reuse counter values because it can cause a break. Since the counter value is used for the encryption for each block as it is processed, if that value was reused for different blocks then it would result in the same ciphertext being created for those blocks and this would result in it becoming less secure. For example, this could result in the plaintext being encrypted into the same ciphertext which would then also compromise the authenticity of the data.

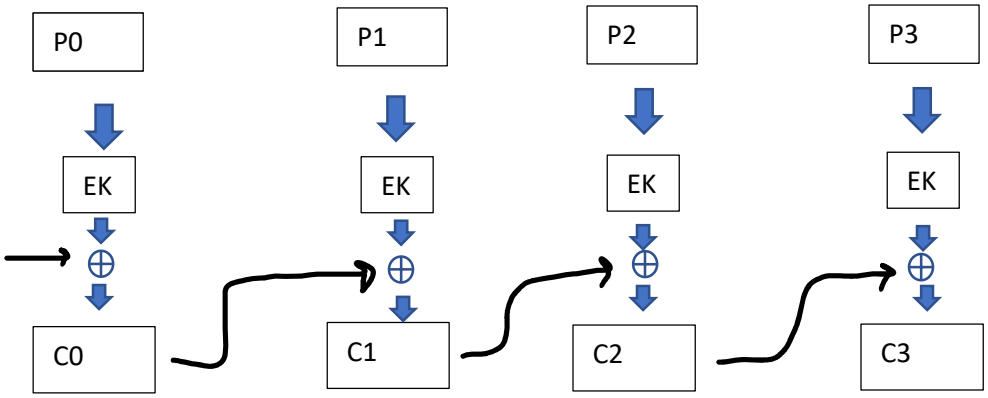
(3) In counter operation mode(CTR) if there is an error in the original encryption or decryption of a block then that same error would correspond in the reverse encryption or decryption of the block. So if the error is there when encryption the data, it would correspond to the same error when that block is then decrypted. This means that there is no error propagation for counter mode because there is no spread of the error, it is isolated to the one block where the error corresponds to. This is because each block is processed with a unique counter value making each block independent from the others. Since they are independent there is no error propagation in counter mode, only the block with the error will be compromised but the rest of the blocks will decrypt as intended. Also, with CTR mode, it can additionally be used with an authentication tag which can help to detect and prevent any outside tampering with the ciphertext.

Assignment 2
Gunnar Yonker

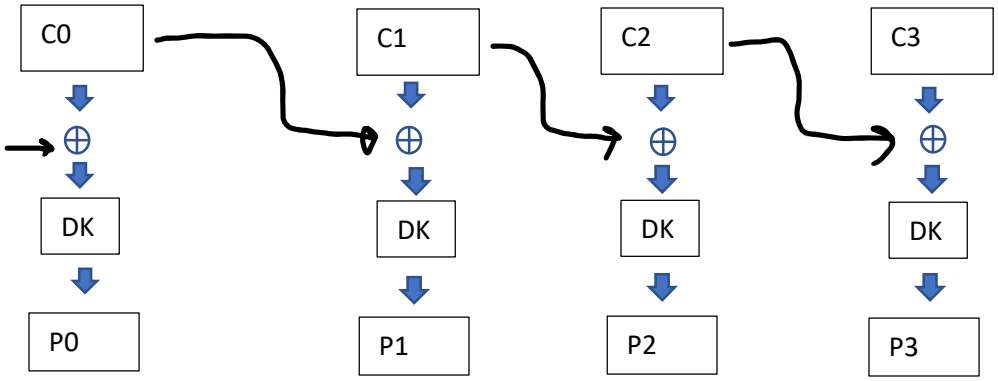
3.

(1)

Encryption:



Decryption:



Decryption formula:

Ci = Ci–1 XOR EK(Pi)

Ci XOR Ci-1 = EK(Pi)

Pi = DK(Ci XOR Ci-1)

DK() = inverse function of EK()

DK = Decryption, EK = Encryption

(2) If an error were to occur to block C3 during the transmission a few plaintexts would be unable to be recovered. This is because the decryption block formula relies on the previous cipherblock text. The receiver would not be able to recover the subsequent plaintext blocks (P3, P4, P5, Pn-1). This is because the decryption formula needs the previous ciphertext block in addition to the encryption key that was applied. So if the error occurred in the C3 block it would then affect the subsequent blocks because the ciphertext being used would no longer be correct due to the error.

Assignment 2
Gunnar Yonker

(3) If there was an error that happened to P3 before encryption, I think that this would cause a propagation error. This would then cause an error in all the subsequent ciphertext blocks(C3,C4,C5…) which would then cause all of the subsequent plaintext blocks including P3 which would contain the original error to be decrypted incorrectly.

(4) Using this block cipher operation mode it would be possible for parallel encryption to be executed because each of the blocks can be encrypted independently using the encryption key(EK) and the previous cipherblock(Ci-1). Decryption using this block cipher mode would not be possible in parallel. This is because during decryption each block depends on the previous decrypted block for the EK (this is seen in Pi-1). So to decrypt each block, you need the previous decrypted block which means that they cannot be run in parallel.

(5) I do not think that this block cipher operation is secure enough for practical usage because it is vulnerable to an attacker being able to modify encrypted messages without being detected. If the attacker changes one of the ciphertext blocks then it can cause an error propagation throughout the whole encrypted message because the plaintext block will change, resulting in the subsequent blocks changing then based on the original modification by the attacker. This greatly impacts the integrity of the message/data because it can be tampered with and would defeat the purpose of the data being encrypted in the first place. Due to the nature of the error propagation within this block cipher operation mode, I don't think that it is sensible to use or secure enough to encrypt/decrypt important data.

4.

(1) B. AddRoundKey

(2) A. Key Length

(3) B. ShiftRows

(4) C. 3, 1

(5) C. The S-box is designed to be resistant to known cryptanalytic attacks.