Review Question:
20.7 What is triple encryption?

Answer: Triple Data Encryption Standard (DES) is a type of computerized cryptography where block cipher algorithms are applied three times to each data block. The key size is increased in Triple DES to ensure additional security through encryption capabilities. Each block contains 64 bits of data. Three keys are referred to as bundle keys with 56 bits per key. There are three keying options in data encryption standards:

1. All keys being independent
2. Key 1 and Key 2 being independent keys
3. All three keys being identical

20.8 Why is the middle portion of 3DES a decryption rather than an encryption?

Answer: There is no cryptographic significance to the use of decryption for the second stage. Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES by repeating the key.

Problems: 20.6, 20.7, 20.10, 20.13 (Part (a) only), 20.14, 20.16
20.6
Answer:

a. No, any block beyond P2 won't be affected. For example, if C1 is corrupted. The output block P3 depends only on the input blocks C2 and C3.
b. All of the ciphertext will totally different with the original ciphertext. At the receiver, the decryption algorithm restores the correct plaintext for blocks except the one in error. Therefore, the error only effects the corresponding decrypted plaintext block.

20.7
Answer:

If an error occurs in a block, it can propagate and all the ciphertext blocks are affected. However, at the receiving end, the decryption algorithm restores the correct plaintext for blocks except the one in error. Therefore, the error only effects the corresponding decrypted plaintext block.

20.10
Answer:
IV is the initialization vector

Mode	Encrypt	Decrypt
CFB	$C_i = E\ (K,\ C_{i-1})\ \oplus P_i$ C_0=IV	P_i= $E\ (K,\ C_{i-1})\ \oplus C_i$
CTR	C_j=$P_j \oplus$(K, counter+j-1)	P_j=$C_j \oplus$(K, counter+j-1)

20.13 a.

Answer: From the first diagram, input initial vector IV XOR with full block P_1. Then, encrypt the result with key K, the output as the input of next block. After encrypting the last full block P_{N-1} it produces the cipher text C_{N-1}. Then, encrypt the cipher text C_{N-1} with key K. In the encryption, select the left most j bits of the encrypted cipher text, and XOR it with the short block to produce the output cipher text. In the last diagram, the last block P_N contains j bits.

20.14

Answer: Totally 9 plaintext characters are affected. First eight is the plaintext characters corresponding to the ciphertext characters. What's more, the altered ciphertext character enters the shift register and is not removed until the next eight characters are processed.

20.16

Answer: The key distribution center operation involves a request from a user to use some service. The KDC use cryptographic techniques to authenticate requesting users as themselves. It checks whether an individual user has the right to access the service requested. If the authenticated user meets all prescribed conditions, the KDC can issue a ticket permitting access. In all, the KDC produces a ticket based on a server key. The client receives the ticket and submits it to the appropriate server. The server can verify the submitted ticket and grant access to user submitting it.