Thomas Hart

CS 465 HW #3

1) P and Q have 100 blocks that are all the same plaintext except 1 bit different in block 10
    a) ECB – each ciphertext block will be the same in P and Q, as each will go through the algorithm without any further manipulation, except for block 10. The 1 different bit in this message block will get stirred up in the encryption process and make the resulting ciphertext block 10 totally different in P and Q.
    b) CBC – every block before block 10 will be the same in P and Q. Because the key is the same, the resulting ciphertext will be the same after encryption and the XOR operation on the next message will also have the same result. After block 10, the different bit will cause changes as it goes through the encryption process, and the XOR of the next message will be different, which will make all the ciphertext blocks after message block 10 totally different for P and Q.
    c) CTR – With the same nonce, key, and counter values, all the resulting ciphertext blocks will be the same in P and Q except for the ciphertext block resulting from the XOR with message block 10. This will only be 1 bit different because the differing bit was not put through the encryption process but just used in the XOR after the nonce/count encryption.
    d) CFB – All the ciphertext blocks will be identical before getting to block 10. Because the ciphertext is created with the nonce encryption result XOR the plaintext, and then used to create the next IV value to be encrypted, all ciphertext blocks after block 10 will be different in P and Q.
    e) OFB – This is almost the same as CFB, except the resulting ciphertext is not used to create the next IV value to be encrypted. It just uses the nonce encryption result. Because of this, the differing plaintext block 10 is not included in further encryptions, and the only difference in P and Q is the one differing bit in block 10 after the XOR with the plaintext.
2) Same as 1 except the nonce is different
    a) ECB – no nonce is used here so it is the same as question 1.
    b) CBC – Because the initial value will XOR with a different nonce in P and Q, every block of ciphertext will be totally different.
    c) CTR – A different nonce in P and Q will cause every encryption to be different, so every ciphertext block will also be totally different.
    d) CFB – A different nonce in P and Q will cause every encryption to be different for this cipher mode too, so all ciphertext blocks will be totally different.
    e) OFB – Same as CFB
3) Same as 1 except its decryption and ciphertext block 25 has a differing bit
    a) ECB – plaintext block 25 will be totally different. The differing bit in ciphertext block 25 will get stirred up in the decryption process and make the block totally different for P and Q. All others will be the same.
    b) CBC – the plaintext in P and Q will be the same for all blocks except for blocks 25 and 26 in the decryption process. Block 25 will be totally different because the differing bit will

go through the decryption algorithm. Block 26 will only be a single bit different because it only needs to XOR with ciphertext block 25. All other blocks will be the same.

c) CTR – The only difference in P and Q here is the 1 bit difference in block 25. You don't have to run the differing bit through the decryption algorithm, so it won't jumble things up. Just encrypt the same using the nonce and counter and then XOR with the ciphertext to get the plaintext again, resulting in a single bit difference.

d) CFB – all plaintext blocks after block 25 will be completely different. The 1 different bit will XOR with the plain text, and the result will be factored into all further encryptions, making P and Q different for all further plaintext blocks. Plaintext block 25 will only be 1 bit different, however, because it only does an XOR with ciphertext block 25.

e) OFB – only 1 bit will be different in plaintext block 25. It will run through the same encryption process, except now the ciphertext will XOR with the results and output the plaintext. The ciphertext is not included in further calculations, so the next blocks won't be affected.

4) Which blocks of ciphertext must be accessed to retrieve plaintext block 50 out of 100 using each cipher mode?
    a) ECB – blocks are not dependent upon each other in this mode to decrypt, so only block 50 needs to be accessed.
    b) CBC – Since all the ciphertext is already known, we can jump to a specific place to decrypt using this mode. We would need ciphertext block 50 to decrypt and also ciphertext block 49 to XOR with to get plaintext block 50.
    c) CTR – plaintext block 50 can be accessed independently of the other blocks. Just run the nonce with the appropriate counter through the algorithm and XOR with ciphertext block 50.
    d) CFB – This mode is like CBC, where we need ciphertext blocks 50 and 49 to get plaintext block 50.
    e) OFB – We need to decrypt everything up until ciphertext block 50 in order to decrypt plaintext block 50 because the ciphertext blocks do not reveal anything to us in the calculations. Each IV is dependent upon the last, so calculate up to block 50, then XOR with the ciphertext to get the plaintext.
5) Which modes permit parallel encryption?
    a) ECB
    b) CTR
6) Which modes permit parallel decryption?
    a) ECB
    b) CBC
    c) CTR
    d) CFB
7) Which modes permit pre-computation of the key stream?
    a) CTR
    b) OFB