Assignment 2 - Cryptography

1. Only 1 key, as sender and receiver use the same key
2. It’s an algorithm whose function is to authenticate both the data and the secret key
3. Plaintext, encryption/decryption algorithm, secret key, ciphertext
4. 1. No, the errors in the block do not propagate
   2. Pn affects C1 which affects Cn, its output, which affects the whole thing, all ciphers, namely Cn
5. 1. Security: 1 loop CBC
   2. Performance: 3 loop CBC
   3. 1 loop CBC is chosen for security because it’s less vulnerable to attacks, and the 3 loop CBC is chosen for performance it can encrypt a lot of blocks with a single key
6. 1. CBC
      1. Encrypt
         1. C1 = E[K, CTR] xor P1
         2. Cj = Pj xor E[K, Cj-1]
      2. Decrypt
         1. P1 = E[K, IV] xor C1
         2. P1 = E[K, Cj-1] xor Cj
   2. CTR
      1. Encrypt
         1. C1 = E[K, CTR] xor P1
         2. Cj = E[K, CTR +j] xor j++
      2. Decrypt
         1. P1 = E[K, CTR] xor C1
         2. Pj = E[K, CTR + j] xor j++
7. 1. Given length of plain text, use CBC to encrypt all but 2 blocks. Perform an xor function against PN-1. Encrypt this new block, select only length of plain text. Pad Pn with zeros and perform exclusive xor with previous encrypted block. Encrypt this last block.
8. For DES, the hash function encrypts and decrypts using the “F” in the DES function which just xors blocks of half block each way.
9. 1. h = 33; f(h) = 20; d = 3, c = 26
   2. h = 55; f(h) = 40; d = 27; x = 14
   3. h = 77; f(h) = 60; d = 53; c = 57
   4. h = 143; f(h) = 120; d = 11; c = 106;
   5. h = 527; f(h) = 480; d = 343; c = 128
10. Yes, if plaintext has n % n, then the encrypted block will have the same. Test both blocks to see if they’re prime. If it is, then divide by n = p or q. If not, factor the blocks using n.