Burrell David
300209541
NWEN243
Assignment 2

1. A plaintext is paired with a secret key. The key is at least as long as the plaintext. The Ciphertext is the bitwise XOR of the plaintext and the key.
   The one-time pad is not that practical, because of how the key must be at least as long as the plaintext, and how hard it is to generate a random number, as well as transportation of the key being problematic.
2. Taking the plaintext and splitting it into blocks and encrypting each of the blocks.
   involves a pipeline of 2 types of transformations (S-box and P-box) and repeating operations until each input bit has an impact on the final output bits. The secret key that is shared between sender and receiver is taken and used to provide confusion, added over several permutations.
3. The purpose of CBC is to avoid having duplicate blocks of ciphertext given the blocks of plaintext are identical. To do this the encryption of each subsequent block in the cipher is dependent on the output of the encryption of the preceding block.
4. The user produces both a public key and a private key, the user shares the public key with everyone and keeps the private key a secret.
   Secrecy: others can encrypt messages with the user's public key, but only they can decrypt them with their private key, making the user the only one who can read the messages.
   Authentication: The user can use their private key to encrypt a message. This message can be read by anyone with access to the user's public key (everyone), however because the user is the only one who could encrypt it so that it can be decrypted with the public key, this makes sure that the message is absolutely from the user.
5. Two giant primes are chosen, p and q.
   $N = pq$
   $Z = (p-1)(q-1)$
   choose some $e < N$ relatively prime to Z.
   public key is (N,e)
   find d such that $(ed) \bmod Z = 1$
   private key is (N, d).
6. Proof: $(m^e \bmod n)^d \bmod n = (m^d \bmod n)^e \bmod n$
   $(m^e \bmod n)^d \bmod n = m^{ed} \bmod n$
   $= m^{de} \bmod n$
   $= (m^d \bmod n)^e \bmod n$
7. The calculations done in the equations take a lot of computation due to the size of the numbers being used and the complexity of the calculations, these also increase with the size of the data being encrypted.
8. To provide secrecy, authentication and message integrity one would create a message signed with your private key (Authenticity), this message is then encrypted using a new symmetric key (integrity) and then the symmetric key to decrypt the message is encrypted using the receivers public key so that only they can decrypt the symmetric key needed to decrypt the message (secrecy)