**21L-6197 Hamza Iftikhar**

Part 1)

In ECB padding ensures that the data length matches the DES block size because in ECB mode data encrypts in the fixed-size blocks 8 bytes for DES algorithm. In the OFB case the padding is not required because it encrypts the data byte by byte.

Part 2)

Because the ECB use the same key for all the block if the block is same the cipher text is also same but on the other side OFB use different key for each part of the plain text so even the plain text is same but the cipher text is different that is why OFB does not reveal so much about plain text.

Part 3)

scrypt(password, salt, key\_len, N, r, p)

* The first one is the password that is provide by user in our case and which is used as the secret to derive the key.
* Salt is a random value that adds uniqueness to the derived key.
* Key\_len is the length if the derived key in bytes.
* N is the CPU/memory cost factor.
* r is the block size parameter.
* p is the parallelization factor.