1. Explain why double DES is not a good idea. (3 points)

> Double DES can be brute forced by meet-in-the-middle attacks to find the intermediate values then they are probably the two keys for encryption stages. In this case, it only provides 57-bit security compared to 56-bits for a single DES, not giving much security increase.

2. Explain two types of Cryptanalysis attacks on AES. (2 points)

> Linear cryptanalysis: known-plaintext attack by finding affine approximations to the cipher's action in which the attack studies the probabilistic linear relation between the key and plaintext parity bits, ciphertext.
>
> Differential cryptanalysis: used to attack stream and block ciphers, in which the attacker studies the difference in information input that can impact the resulting differences in the output.

3. Research and describe the five types of operations in block cipher modes, ECB (Electronic Code Block) mode, CBC (Cipher Block Chaining) mode, CFB (Cipher Feedback) mode, OFB (Output Feedback) mode, and CTR (Counter) mode. (5 points)

> ECB mode: use a block cipher to encrypt long messages. Divide into blocks and encrypt independently.
>
> CBC mode: the output of the previous cipher is given as input to the next cipher block by XOR the input of the next cipher block.
>
> CFB mode: Use initial vector for first encryption and output in s bits and b bits. s is used for XOR with messages and the output is used as s and the output goes to a shift register with the position of s and b changed.
>
> OFB mode: encrypt the initial vector first. the output is used for encrypting first-part messages and also send to the next stage to repeat the process.
>
> CTR mode: counter-based block cipher. Each block uses a counter-initiated value to encrypt first and encrypt plaintext by XOR, which can be implemented in parallel.