Lab1: Secret Key

Task 1: Frequency Analysis [6 Marks]

1. Why monoalphabetic substitution cipher is not secure?
2. Please do the steps mentioned in the lab instruction and provide your decrypted result and screenshots here.

Task 2: Encryption using Different Cipher and Modes [11 Marks]

1. What are the differences between CBC, OFB, CRT cipher mode based on table below?

	Plaintext file size	Encrypted file size
ECB	26	
CBC	26	
OFB	26	

2. Are the sizes of plaintext and ciphertext different? Explain Why?
3. Please follow the task 2 instruction and provide your screenshots of 3 different modes of operations here.

Task 3: Encryption Modes – ECB vs. CBC [8 Marks]

1. What is the difference between ECB and CBC mode?
2. Which modes do you think perform better in encrypting the image? Why?
3. Please follow the task 3 instruction and provide your screenshots for task 3 here.

Task 4: Padding [4 Marks]

1. Which modes of operations used padding and which ones not? Why?
2. Please follow the task 4 instruction and provide your screenshots for task 4 here.

Task 5: Error Propagation – Corrupted Cipher Text [4 Marks]

1. What is Error propagation means?
2. Which mode of operation is worse in error propagation? Why?
3. Please follow the task 5 instruction and provide your screenshots for task 5 here.

Task 6: Initial Vector (IV) and Common Mistake [10 Marks]

1. What characteristics make IV secure?
2. Which mode of operation is not using IV? how can make it more secure?
3. What is chosen-plaintext attack? What Mistake in IV can cause chosen-plaintext attack?
4. What is known-plaintext attack? what mistake in IV can cause this type of attack?
5. How could we compromise a message when we have ciphertext, IV makes that cipher text, and the Next IV (as we predict it)? (**Hint**: for this question you need to figure out task 6.3 and explain here what steps you need to took to find out the plaintext) [4 Marks – 1 Mark for each step]

Task 7: Programming using the Crypto Library [5 Marks]

1. If you are given a plaintext and ciphertext, how can you find the key that is used for encryption when you know the following facts:
    a. The aes-128-cbc is being used for encryption
    b. The key is English word shorter than 16 characters

    Note: you can either write a program to do this task and provide the screenshot of your result or just explain how you can solve it.