Lab Final Examination – Summer 2026
Course Code: CIS311L (Batch 20A)
Course Title: Network Security and Cryptography Lab
Set: **B** Date: 10.08.2026

Time: 1 Hour Total Marks: 2 x 20 = 40

[Select any **ONE** question from each part and answer it.]

Write the program using either Python or JavaScript. Include the appropriate output for each program.

Part 1:

a. Write a program that processes the string **"Hash Function"** and performs a **bitwise OR** operation on each character using the key value **170**. For each character, convert it to its ASCII value, display the ASCII value in hexadecimal format, perform the XOR operation, and display the XOR result in decimal, binary, and character format.
b. Implement the **AES-192** symmetric encryption algorithm in **CBC mode**. The program should encrypt the plaintext **"Confidential Report"**. Decrypt the ciphertext using the same key and IV, and display the plaintext, generated key, key size, ciphertext, and decrypted plaintext.

Part 2:

a. Implement the SHA-256 hashing algorithm to generate the hash of the plaintext **"Accountability, Access Control, Authorization, Data Protection"** using both the complete message and the message divided into multiple **(6 chunks)** parts. Display the original plaintext, both generated hash values, the length of each hash, and compare the outputs to verify that both approaches produce the same hash.
b. Write a program that takes the plaintext **"Digital Forensics Lab"** and the key **47** as input. Encrypt the plaintext using the Caesar Cipher algorithm, then decrypt the generated ciphertext using the same key. Display the original plaintext, ciphertext, ciphertext length, and decrypted plaintext.

Important Instructions:

- Create a folder on Desktop and rename it using your **Student ID_Set** ***(e.g., 242-16-002_SetB)***. **Please follow this format strictly.**
- Save all your source code files inside this folder.
- In each source code file, include your Student ID as a comment at the beginning of the file.