Course : Introduction to Cryptography (ITC)

Session: July - Dec 2025

LAB ASSIGNMENT - 4

Deadline: 17-November-2025 (Monday) Midnight

Objective

To understand how native C code can be compiled to WebAssembly (WASM) and executed in the browser using JavaScript (Next.js).
You will implement a simple RC4 encryption/decryption system, where the core algorithm is written in C, compiled to WASM, and invoked from the browser frontend.

Learning Outcomes

By the end of this lab, students will learn:

1. **How to compile C code to WebAssembly using Emscripten.**

2. **How to expose C functions to JavaScript.**

3. **How to call native C (via WASM) from a Next.js frontend.**

4. **How to handle text input/output between JavaScript and WASM memory.**

Step 1: Implement the RC4 Algorithm in C

Write an RC4 implementation in C (from scratch - don't use any crypto library).
Your file should be named "rc4.c".

Part 2: Compile to WebAssembly

Use **Emscripten** to compile your C code into a `.wasm` module.

Part 3: Create the Next.js Frontend

Requirements:

- Two textboxes:
    - One for the **plaintext/ciphertext**

    - One for the **key**

- Two buttons:
    - **Encrypt:** encrypts the given text using the given key using RC4 wasm code
    - **Decrypt:** decrypts the given text using the given key using RC4 wasm code

- One display area for the result.

END