ByteCrypt

Introduction to Computers and Programming in C (ES202)

Project Presentation

Creator: Aayan Khan

Section: 1CSE-1Y

Enrolment No.: A2305225054

Batch: 2025-29

Teacher: Dr. Ashish Mani

Key Questions

What?

How?

Why?

What is ByteCrypt?

Description

- A C-based project capable of encrypting and decrypting files by performing direct bit-level manipulation of their data.
- The process works by having the user provide a password to secure the document, which generates a corresponding key for use.
- The files can essentially be of any data type, such as audio, plain text, video, or even PDFs.

Demonstration

Plain Text File

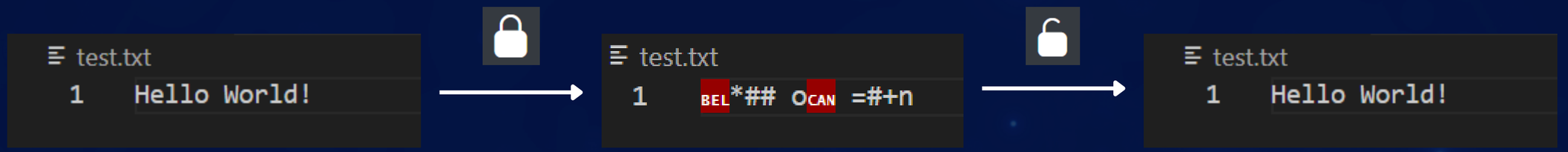
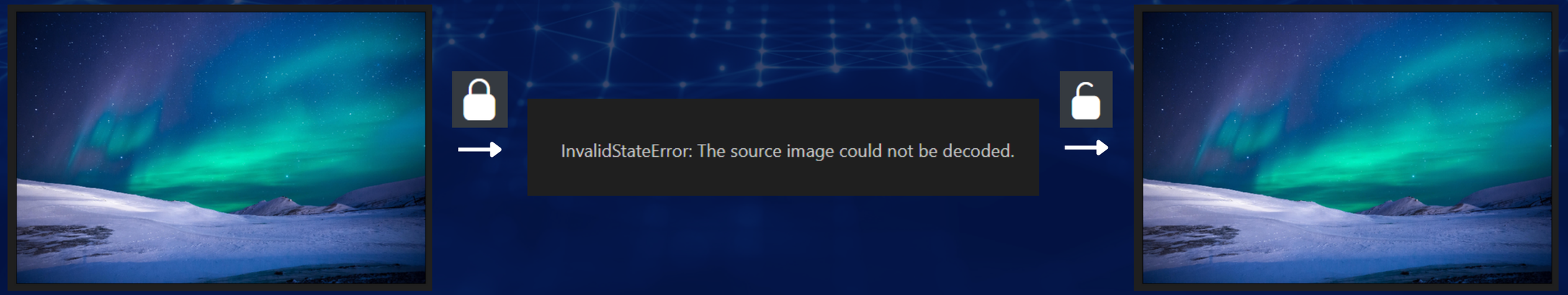
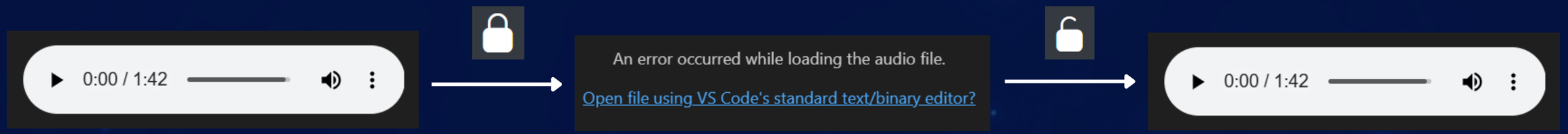


Image File

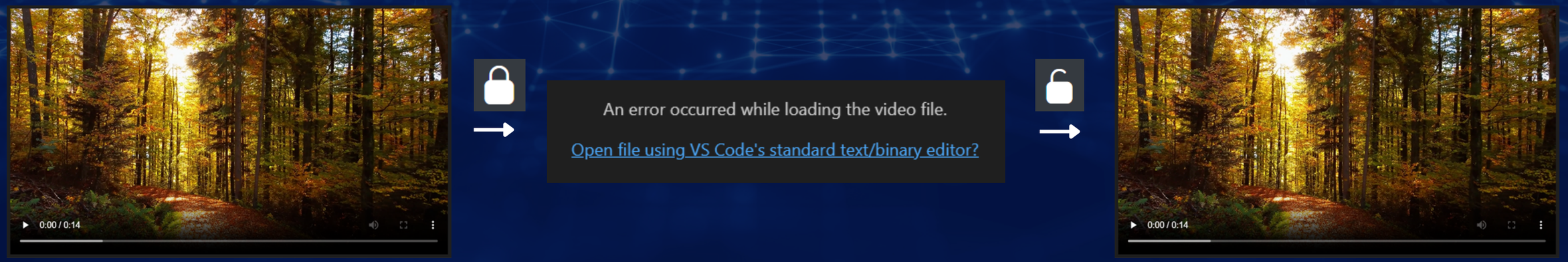


Demonstration

Audio File

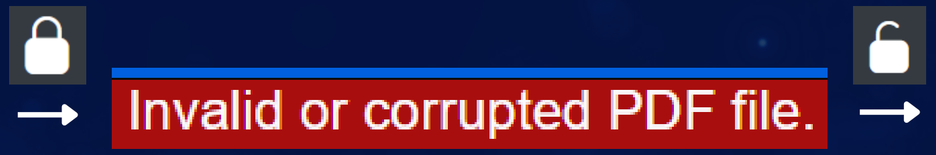


Video File

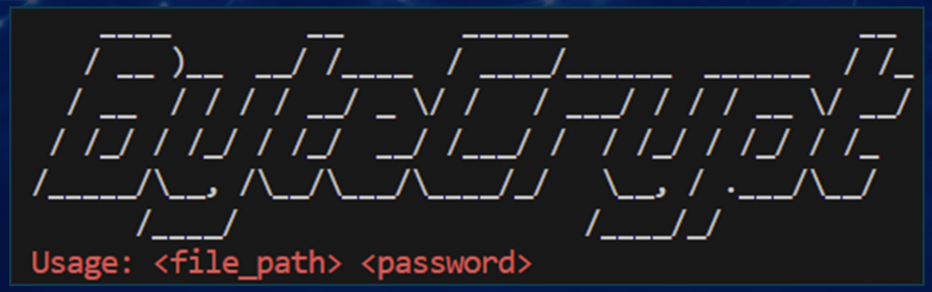


Demonstration

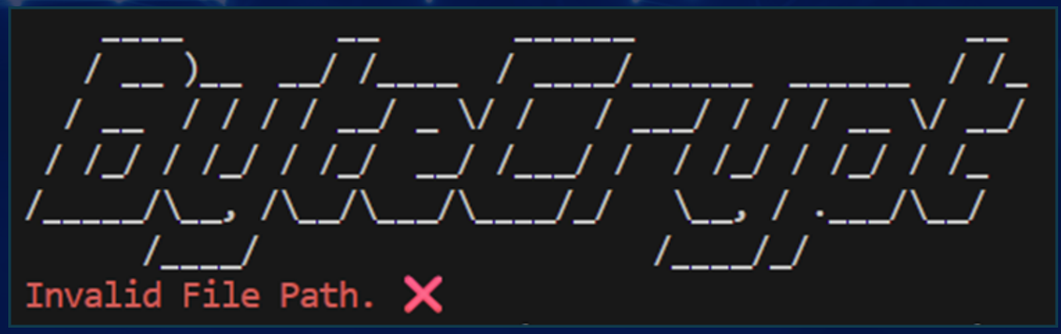
PDF File



#Invalid Usage



#Invalid File Path Provided



How does it work?

Generating the Key

- The user enters a password along with the file path through the CLI.
- The Daniel Bernstein Rolling Algorithm is used to generate the key.
- The algorithm entails:
  - A base key value of 5381
  - A multiplier variable (33)
  - For each char in password
    - key = key * multiplier + (int) char;
  - Return key % 256

How does it work?

Securing the File

- The file is opened in binary read-write mode.
- An infinite loop is started:
  - A chunk buffer of 4096 bytes is created.
  - Data is read from the file, with the number of bytes read stored in a variable n.
  - If n is 0, EOF → break the loop.
  - For each byte in the chunk
    - chunk[byte] = chunk[byte] ^ key;
  - Pointer moves backwards by n bytes.
  - Modified chunk is written back.
  - Changes are flushed.
- The file is closed.

Why?

- The primary motivation was to create a simple, fast, and accessible method for securing files on local systems.
- This thereby reduced reliance on heavy external tools or complex cryptographic libraries.
- By utilizing XOR-based encryption with a password-derived key, this project provides an easy-to-understand and platform-independent approach to file protection.

Thank You