HKBK COLLEGE OF ENGINEERING

**Department of Information Science and Engineering**

**PROJECT PROPOSAL – 6th Semester**

**18ISL67 – File Structure Lab (Part- B)**

**Mini Project**

|  |  |
| --- | --- |
|  | **Project Title:** File Encryption and Decryption |
|  | **Branch:** ISE  **Sem & Sec:** 6-B |
|  | **Relevance-**   * + - 1. **Document Processing,**       2. **Transaction Management,**       3. Indexing and Hashing,       4. Buffer Management,       5. Configuration Management |
|  | **Name(s) of project guide(s):**   1. **Name:**   **Designation:**  **Email id:**  **Contact No.:** |
|  | **Name of Team Members**  **Name:** Syeda Umme Kulsum  **USN No.:** 1HK20IS110  **Email id:** 1hk20is110@hkbk.edu.in  **Mobile No:** 8217219556    **Name:** Umme Hania **USN No.:** 1HK20IS119  **Email id:** 1hk20is119@hkbk.edu.in  **Mobile No:** 8310760065 |
|  | **Date of commencement of the Project:** |
|  | **Abstract of the project:**  **Abstract 1:**  The program is a file encryption and decryption tool that uses a structured file system to organize and manage files. The program allows users to select a file to encrypt or decrypt and specifies a password for encryption. The program utilizes a secure encryption algorithm to encrypt the file, making it inaccessible to unauthorized users. The encrypted file is then saved in the structured file system, where it can be easily accessed and managed by the user.When the user wants to decrypt the file, they select the encrypted file and enter the password used for encryption. The program decrypts the file using the same encryption algorithm and password, and saves the decrypted file back to its original location in the structured file system.The program also includes additional features such as the ability to rename, move, or delete files in the structured file system, as well as search and sort files based on various criteria. Overall, the program provides a secure and user-friendly way to encrypt and manage files with a structured file system.  **Abstract 2:**  File encryption and decryption are important techniques for protecting sensitive information from unauthorized access. The AES (Advanced Encryption Standard) algorithm is widely used for file encryption and decryption due to its security, efficiency, and flexibility.AES uses symmetric key encryption, which means that the same key is used for both encryption and decryption. The key length can vary from 128 to 256 bits depending on the level of security required. AES operates on fixed-size blocks of data, with a block size of 128 bits.To encrypt a file using AES, the plaintext data is divided into blocks and each block is processed using a round function that involves substitution, permutation, and XOR operations. The key is used in each round to create a different ciphertext for each block. The resulting ciphertext is then transmitted or stored securely.To decrypt a file encrypted with AES, the reverse process is performed. The ciphertext is divided into blocks and each block is processed using the inverse of the round function with the same key. The resulting plaintext is then reconstructed.AES has become a widely accepted standard for file encryption and decryption due to its strength, speed, and flexibility. Its use is recommended for securing sensitive information in a variety of contexts, including financial transactions, healthcare records, and military communications. |
|  | **Objectives of the project:**   1. Confidentiality of the files 2. Integrity of its contents 3. Authorization |
|  | **Methodology of work:**   * User selects a file to encrypt: The user chooses a file they want to encrypt, such as a document or a photo. * Encryption process begins: The program uses a secure encryption algorithm to transform the file into an unreadable format. This may involve converting the file into a binary format, and then applying a series of mathematical operations to it. * Encrypted file is stored in the file structure: Once the encryption process is complete, the encrypted file is stored in the file structure. This may involve creating a new directory for encrypted files, or adding the encrypted file to an existing directory. * User can manage encrypted files: The user can now manage the encrypted file using the file structure. This may involve moving the file to a different directory, renaming it, or deleting it. * User selects a file to decrypt: When the user wants to access the original file, they select the encrypted file from the file structure. * Decryption process begins: The program uses the same encryption algorithm to reverse the encryption process and restore the file to its original format. This may involve applying a series of mathematical operations to the encrypted file to convert it back into a readable format. * Decrypted file is stored in the file structure: Once the decryption process is complete, the decrypted file is stored in the file structure. This may involve creating a new directory for decrypted files, or adding the decrypted file to an existing directory. * Overall, a program that uses file structure and encrypts and decrypts a file provides a secure and organized way to protect sensitive files from unauthorized access. The file structure allows users to easily manage and organize their encrypted files, while the encryption algorithm ensures that the files remain unreadable to anyone who does not have the proper decryption key. |
|  | **Expected Outcome of the project:**  Implementation of a file structure for encryption and decryption of a file |
|  | **Specify Relevance to PO/PSO :**  PO1, PO2, PO3, PO4, PO5, PO6, PO9, PO10, PO11, PO12, PSO1, PSO2, PSO3, PSO4 |
|  | **Reference:**   * Computer networks textbook * Python programming language * Google and you tube resources |
|  | **Project Coordinator:**  **Name:**Dr.V.Balaji Vijayan  **Email id:**balaji.is@hkbk.edu.in  **Contact No.:** +91 9943397400  **Name:** Prof.Sharavana K  **Email id:** sharavanak.is@hkbk.edu.in  **Contact No.:** +91 9902054977 |

|  |  |  |
| --- | --- | --- |
| **Project Guide** | **Project Coordinator** | **HOD** |
|  | **Dr.V.Balaji Vijayan**  **Prof. Sharavana K** | **Dr.A.Syed Mustafa** |

**Note:**

**Remove All Comments/Note Specified in Bracket (…..) before Submission**

**Annexure A**

**PROGRAM OUTCOMES (POs)**

**Computer Science and Engineering Graduates will be able to:**

1. **Engineering knowledge:** Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.
2. **Problem analysis:** Identify, formulate, review research literature, and analyse complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.
3. **Design/development of solutions:** Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.
4. **Conduct investigations of complex problems:** Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.
5. **Modern tool usage:** Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modelling to complex engineering activities with an understanding of the limitations.
6. **The engineer and society:** Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.
7. **Environment and sustainability:** Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.
8. **Ethics:** Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.
9. **Individual and team work:** Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.
10. **Communication:** Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.
11. **Project management and finance:** Demonstrate knowledge and understanding of the engineering and management principles and apply these to one’s own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.
12. **Life-long learning:** Recognize the need for, and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

**PROGRAM SPECIFIC OUTCOMES (PSOs)**

1. **Professional Skills:** An ability to identify and analyze requirements, and in designing and implementing well-tested technology solutions for rapidly changing computing problems and information system environments.
2. **Problem-Solving Skills:** An ability to Design, develop and optimize solutions for information systems employing fundamentals of system hardware & software, graph theory, finite automata, data storage and   
   communication networks.
3. **Collaborative Skills:** An ability to communicate and develop leadership skills, and work effectively in team environments. They are capable of collaborating to design and implement well- tested solutions for rapidly changing computing problems and information system environments.
4. **Successful Career and Entrepreneurship Skills:** An ability to adapt for innovation and changes and be successful in ethical professional careers along with the impact of computing on society, and platforms in creating innovative career paths to be an entrepreneur, and a zest for higher studies.