TITLE: DATA ENCRYPTION AND DECRYPTION SYSTEM

Abstract:

The "ImprovedVersionOfMain" Java program exemplifies secure data encryption and storage using the Advanced Encryption Standard (AES) algorithm, while emphasizing robust key management practices.

The program allows users to input a message, encrypt it, and then decrypt it, demonstrating data protection with encryption keys stored in a KeyStore.

Key Features:

1) User Interaction: *The program interacts with the user, allowing them to input a message to be encrypted and later decrypted.*

2) AES Encryption: *It employs the AES encryption algorithm to secure the user's data. AES is a widely accepted encryption algorithm that provides strong data protection.*

3) *Key Management: The program utilizes a KeyStore to securely manage the encryption keys.*
   It generates a random AES key, stores it in the KeyStore, and subsequently retrieves the key for data encryption and decryption.

4) *Dynamic Key Generation: If the KeyStore does not exist, the program creates one and generates a new AES encryption key.*
   It ensures that a valid key is always available for secure operations.

5) *Data Integrity: The program maintains data integrity by verifying that the stored key is of the correct type (SecretKey) before use.*

6) *File Persistence: The generated KeyStore and keys are persisted in a file ("keystore.jceks") to ensure data and key retention across program runs.*

7) *Base64 Encoding: Before display, the encrypted data is converted to Base64 format, enabling it to be safely printed and decoded.*

8) *Exception Handling: The program provides error-handling and informative error messages to guide users in case of issues.*

Conclusion:

This code can serve as a foundation for secure data storage and retrieval in applications that require data confidentiality.

It showcases essential practices in key management and data encryption, enabling users to apply these techniques to enhance the security of their applications.