**File Encryption and Decryption using AES in Python**

This Python program allows users to securely encrypt and decrypt files using the AES (Advanced Encryption Standard) algorithm in CBC (Cipher Block Chaining) mode.

The code is organized into the following major steps:

1. Key Generation

generate\_key() function creates a strong, random 32-byte encryption key using get\_random\_bytes(32).

This key is needed for both encryption and decryption.

The key is saved into a file called key.bin for future use.

2. Key Loading

load\_key() function reads the encryption key from the key.bin file.

This loaded key is later used in encrypting or decrypting files.

3. File Encryption

encrypt\_file(file\_path, key) does the following:

Reads the contents of the specified file.

Adds padding to the data (so that the total size becomes a multiple of 16 bytes — required by AES).

Creates a cipher using the loaded key and a random Initialization Vector (IV).

Encrypts the file data.

Saves the encrypted data along with the IV into a new file (with .enc extension).

The IV is important for decryption and is stored inside the encrypted file itself.

4. File Decryption

decrypt\_file(encrypted\_path, key) does the reverse:

Reads the encrypted file.

Extracts the first 16 bytes as the IV.

Uses the IV and key to create the same cipher used for encryption.

Decrypts the data.

Removes the padding to retrieve the original data.

Saves the decrypted file with a name ending in \_decrypted.

5. Main Program Flow

The program first shows a menu:

Option 1: Generate a new key.

Option 2: Encrypt a file using an existing key.

Option 3: Decrypt an encrypted file.

Based on user input, it performs the selected action.

📌 Important Notes

AES-256 encryption is used (because the key size is 32 bytes = 256 bits).

Padding ensures that the file's data fits AES block size requirements.

IV is random for each encryption, making the encryption more secure even if the same file is encrypted multiple times.

Security Warning: The key.bin file must be protected. If someone steals it, they can decrypt your files.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**AES File Encryption and Secure Deletion**

This Python script performs two key tasks:

**Encrypts a file using AES encryption (CBC mode)**

**Securely deletes the original file by overwriting it with random data** before removing it

**Code Breakdown**

1. **AES Encryption**

**AES Setup:**

The script uses **AES-256** encryption, which means a **256-bit key** (KEY = os.urandom(32)) and a **128-bit initialization vector (IV)** (IV = os.urandom(16)).

The Cipher class from cryptography is used for the AES encryption process.

**CBC mode** is employed, meaning the encryption of each block depends on the previous block, and an IV is required for this mode.

**Encryption Process:**

**Padding:** AES operates in fixed-size blocks (16 bytes). If the file data isn't a multiple of 16 bytes, padding is added to ensure the data fits perfectly.

**Cipher Initialization:** A cipher object is created using the AES algorithm, CBC mode, and the generated IV.

**Encryption:** The plaintext file is encrypted using the cipher, producing **ciphertext** (the encrypted file data).

The **IV** is prepended to the encrypted data before saving it. The IV must be stored with the encrypted content because it is required for decryption.

**Saving the Encrypted File:**

The encrypted data is saved in a new file with a .encrypted extension.

2. **Secure File Deletion**

**Secure Deletion Process:**

Before deleting the original file, it is overwritten with **random data** (os.urandom(filesize)) to make sure that sensitive information is not recoverable.

The original file is then deleted using os.remove(filename).

**Why Overwrite?**  
Overwriting the file with random data ensures that the original content cannot be restored even with advanced data recovery methods.

**Main Flow**

**User Input:**  
The program prompts the user for the file path of the file they want to encrypt and securely delete.

**Validation:**  
The script checks if the file exists using os.path.exists(). If the file is found, it proceeds with encryption and deletion. If not, it alerts the user.

**Actions Taken:**

**Encrypt the File:** The encrypt\_file(filename) function encrypts the file using AES and saves it with the .encrypted extension.

**Securely Delete the File:** The securely\_delete\_file(filename) function overwrites the file with random data and then deletes it.

**Security Considerations**

**Encryption (AES-256):** AES-256 is one of the strongest encryption algorithms available today, making it suitable for protecting sensitive data.

**Secure Deletion:** Simply deleting a file doesn’t ensure it’s gone — it can be recovered with specialized software. Overwriting the file with random data and then deleting it ensures that the data cannot be easily recovered.

**Summary of Features**

**Encryption:** AES-256 in CBC mode with random IV.

**Secure Deletion:** Overwrites the file with random data before removal.

**File Handling:** Reads and writes files with correct handling of padding and encryption/decryption steps.

**Potential Improvements:**

**Key Management:** Currently, the encryption key is generated randomly and stored only in memory, meaning you lose the ability to decrypt the file once the program ends. You could save the key securely for later use.

**Decryption Functionality:** You could implement a decryption function where the user can decrypt files using the same AES key.

**Error Handling:** More robust error handling, such as verifying the file's integrity before deletion, would improve the script.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

**Key Generation and Loading Script for AES Encryption**

This Python script helps you **generate AES keys** for encryption and **load existing AES keys** from saved files. It demonstrates basic file handling for **key management** in AES encryption systems. Let’s break it down:

**Key Concepts**

**AES Key Generation:**

**AES (Advanced Encryption Standard)** is a symmetric encryption algorithm, and to encrypt or decrypt data with AES, you need a secret key.

This script generates a **256-bit AES key** (which is 32 bytes) using os.urandom(32), ensuring a cryptographically secure random key.

**Key File Management:**

The script can **save the AES key** to a file and **load it back** when needed. This is useful for cases where you want to store the key separately and later use it for encryption or decryption.

The keys are saved with filenames like aes\_key\_1.bin, aes\_key\_2.bin, etc. The index is provided by the user to ensure multiple keys can be stored and loaded as needed.

**Functions Breakdown**

1. generate\_and\_save\_key(index):

**Purpose:** This function generates a new **random AES key** and saves it to a file with a name based on the provided index (e.g., aes\_key\_1.bin).

**Key Generation:**  
os.urandom(32) generates a 256-bit (32-byte) random key, suitable for AES-256 encryption.

**File Writing:**  
The key is written to a binary file using wb mode, meaning it writes raw bytes directly.

2. load\_key(index):

**Purpose:** This function loads an existing AES key from a file with the given index (e.g., aes\_key\_1.bin).

**File Checking:**  
The function first checks if the file exists using os.path.exists(). If the file is found, it reads the key bytes from the file and returns them.

If the file does not exist, the function prints an error message and returns None.

**Main Program Flow**

**User Input:**

The program asks the user whether they want to **generate and save a new key** or **load an existing key**.

Depending on the user’s choice, the program will either:

**Generate a new key** and save it to a file, or

**Load an existing key** from a file and print the key (in hexadecimal format).

**Choice Validation:**

The user’s choice is validated: it must be either 'G' (for generate) or 'L' (for load). If an invalid option is selected, the program will print an error message.

**Key Display:**

If a key is successfully loaded, the key is displayed in **hexadecimal format** using key.hex(). This format is often used to represent binary data in a human-readable form.

**Use Case and Applications**

**Generating AES Keys:** This can be used as part of an encryption system where each user or session has a unique key stored securely.

**Loading AES Keys:** Loading keys from saved files is useful for decrypting files or continuing encryption operations across multiple runs of the program.

**Secure Key Storage:** The saved .bin files need to be securely stored since possession of the key is crucial for decrypting any encrypted data.

**Security Considerations**

**Key Protection:** The generated keys should be kept secure. If someone has access to the key file, they can decrypt any data encrypted with that key.

**Key Backup:** Ensure that important keys are backed up securely in case they are needed for decryption in the future.

**Example Workflow:**

**Generate Key:**

User selects **'G'** to generate a new key, enters an index (e.g., 1), and the AES key is saved as aes\_key\_1.bin.

**Load Key:**

User selects **'L'**, enters the index (e.g., 1), and the program loads the key from aes\_key\_1.bin, displaying it as a hexadecimal string.

**Improvements or Extensions**

**Key Encryption:** You could encrypt the AES keys themselves for additional security before saving them, especially if the keys are stored in less-secure locations.

**Key Management System:** A system to list all saved keys, delete keys, or check key integrity could be added to improve usability.  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
**Symmetric Encryption and Decryption with Password-based Key Derivation**

This Python script demonstrates **AES encryption and decryption** using a **password** to derive the encryption key. It uses **PBKDF2 (Password-Based Key Derivation Function 2)** for securely deriving a strong encryption key from a password, combined with AES encryption in **CBC (Cipher Block Chaining) mode**.

**Key Components:**

**Key Derivation with PBKDF2:**

The password provided by the user is transformed into a strong encryption key using **PBKDF2**.

PBKDF2 is a key derivation function that uses a password, a salt, and an iteration count to generate a secure encryption key. This process ensures that even if two users have the same password, their keys will be different due to the use of **salt**.

The **salt** is randomly generated each time, providing additional security against precomputed attacks (e.g., rainbow tables).

**AES Encryption and Decryption:**

**AES (Advanced Encryption Standard)** is a symmetric encryption algorithm used to encrypt and decrypt messages.

The AES key is derived from the password, and **CBC mode** is used for encryption. In CBC mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted, ensuring that identical plaintext blocks produce different ciphertext blocks.

An **Initialization Vector (IV)** is also randomly generated for each encryption to ensure the ciphertext is unique even when the same plaintext is encrypted multiple times with the same key.

**Functions Breakdown:**

1. derive\_key(password, salt):

**Purpose:** Derives a 32-byte AES encryption key from the given password and salt using **PBKDF2**.

**PBKDF2 Parameters:**

password: The password provided by the user (encoded to bytes).

salt: A random 16-byte salt (ensures unique keys for identical passwords).

dkLen=32: The length of the derived key (32 bytes = 256 bits for AES-256).

count=390000: The number of iterations, which makes the key derivation slower, improving security.

2. encrypt\_message(message, password):

**Purpose:** Encrypts a message using AES encryption with a password-derived key.

**Process:**

**Salt Generation:** A random 16-byte salt is generated.

**Key Derivation:** The password and salt are used to derive the AES key.

**Padding:** The message is padded to ensure it is a multiple of 16 bytes (required by AES).

**Encryption:** The message is encrypted with AES in CBC mode, using the derived key and a randomly generated IV.

**Encoding:** The salt, IV, and encrypted message are concatenated and base64-encoded for easy storage or transmission.

3. decrypt\_message(encrypted\_blob, password):

**Purpose:** Decrypts an encrypted message using the password-derived key.

**Process:**

**Decoding:** The base64-encoded encrypted blob is decoded into the salt, IV, and encrypted message.

**Key Derivation:** The password and salt are used to derive the same AES key as used during encryption.

**Decryption:** The message is decrypted using AES in CBC mode with the derived key and the IV.

**Padding Removal:** The padding added during encryption is removed to restore the original message.

**Main Program Flow:**

**User Input:**  
The program offers the user a choice to either encrypt or decrypt a message:

**Encrypt:** The user provides a plaintext message and a password. The message is encrypted using AES with the derived key, and the encrypted message is displayed.

**Decrypt:** The user provides an encrypted message (base64 encoded) and the correct password. If the password is correct, the encrypted message is decrypted and displayed.

**Error Handling:**  
If decryption fails (for instance, due to an incorrect password), an error message is displayed.

**Security Considerations:**

**Password-based Key Derivation:**

The use of **PBKDF2** with a random salt ensures that the key derivation is secure. It makes brute-force attacks computationally expensive by requiring many iterations to derive the key.

**Encryption with AES-256:**

AES with a 256-bit key is very secure and is widely used in secure communications and data protection systems.

**Random Salt and IV:**

The salt and IV are generated randomly for each encryption. This prevents patterns in encrypted data and ensures that even the same message encrypted multiple times with the same password will have different ciphertexts.

**Example Workflow:**

**Encrypting a Message:**

The user chooses to encrypt a message and provides the message and a password.

The program encrypts the message and returns the encrypted message in base64 format.

**Decrypting a Message:**

The user pastes the encrypted message (base64) and provides the password.

If the password is correct, the program decrypts the message and displays it.

**Improvement Ideas:**

**Key Storage:**  
For better security, instead of using the password directly each time, you could store the key (or its hash) securely after the first use, so users don’t have to input the password repeatedly.

**Password Strength Checking:**  
It might be a good idea to implement a password strength check, ensuring users choose sufficiently strong passwords.

**Error Handling in Encryption:**  
More detailed error handling could be added, such as checking for empty input fields and invalid characters in the message.  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*  
  
1. **AES File Encryption and Decryption (First Code)**

**Purpose:** Encrypt and decrypt files using AES encryption.

**Applications:**

**Secure File Storage:** This code can be used for securely encrypting sensitive files before storing them on a local system or cloud storage, preventing unauthorized access.

**Backup Encryption:** When creating backups of sensitive information (e.g., financial records or personal documents), this encryption ensures that even if the backup is compromised, the data remains unreadable without the decryption key.

**Data Transfer Security:** It can be used to encrypt files before transferring them over insecure networks (e.g., via email or FTP), ensuring data confidentiality.

**Compliance with Data Protection Regulations:** Organizations can use this encryption for complying with data protection laws (like GDPR or HIPAA) by encrypting sensitive personal data.

2. **File Deletion with Secure Erasure (Second Code)**

**Purpose:** Encrypt and securely delete files.

**Applications:**

**Secure File Deletion:** This is used in situations where you need to ensure that sensitive files (e.g., financial data, personal information, or company secrets) are completely deleted and cannot be recovered by unauthorized parties. The method overwrites files before deletion, which is critical in fields requiring high security, like cybersecurity and IT compliance.

**Data Privacy:** It ensures that data from old or decommissioned systems is fully erased, which is important in organizations that need to follow data privacy laws (such as GDPR, CCPA).

**Forensic Data Destruction:** It can be applied in scenarios where organizations must guarantee that no data can be recovered from discarded or decommissioned drives (e.g., when decommissioning hardware).

3. **Key Generation and Management (Third Code)**

**Purpose:** Generate, save, and load AES keys for file encryption.

**Applications:**

**Key Management in Encryption Systems:** This code is crucial in building systems that involve symmetric encryption (like AES). It ensures that AES keys are securely stored and managed.

**Encryption-as-a-Service (EaaS):** Cloud services that offer file encryption (or other forms of data encryption) often need to securely generate, store, and load encryption keys for clients.

**Secure Key Storage Solutions:** It can be extended to create a key management system that securely stores and retrieves encryption keys from a database or hardware security module (HSM), preventing unauthorized access.

4. **Password-Based Encryption and Decryption (Fourth Code)**

**Purpose:** Encrypt and decrypt messages using AES with password-derived keys.

**Applications:**

**Secure Messaging Systems:** This can be integrated into messaging platforms that require end-to-end encryption, ensuring that only the intended recipient with the correct password can decrypt the message.

**Password-Based File Encryption:** Similar to the file encryption code, but in this case, a user-provided password (rather than a pre-shared key) is used for encryption, which is useful in scenarios where users want to control their encryption keys.

**Personal Security Applications:** It can be used in applications where users need to protect sensitive messages or documents with a password (e.g., encrypting email content or personal notes).

**Data Protection for Personal Use:** People can use this script to protect private files (e.g., personal diaries, photos) by encrypting them with a password that only they know.

**Secure Online Transactions:** In e-commerce or banking applications, this technique can ensure that user credentials and sensitive transaction information are encrypted before sending over the internet.

5. **AES Key Generation and Loading (Fifth Code)**

**Purpose:** Generate and load AES keys based on an index.

**Applications:**

**Multi-Key Encryption Systems:** This approach allows for generating and using multiple keys based on an index. It can be useful in systems that need to rotate encryption keys periodically for added security.

**Key Management for Distributed Systems:** This can be useful in distributed systems (e.g., cloud storage, blockchain systems) where different nodes or users need to manage different keys.

**Security Systems with Multiple Access Levels:** In some applications, different users or access levels may need different encryption keys for different sets of data (e.g., corporate data with different access controls).

6. **Message Encryption with Password (Sixth Code)**

**Purpose:** Encrypt and decrypt messages using a password-derived key (PBKDF2 + AES).

**Applications:**

**Password-based Secure Communication:** This is highly applicable in messaging apps that use password-based encryption, ensuring the message is encrypted with a key derived from a user-provided password.

**Secure Online Communication Platforms:** It can be implemented in platforms that require the protection of communication, such as email services or chat apps that guarantee confidentiality.

**Secure Document Sharing:** It can be used in applications that allow users to send encrypted documents or messages, requiring a password for decryption.

**Data Protection in Cloud Storage:** Users can encrypt sensitive data before uploading it to cloud storage and provide a password to decrypt it whenever necessary.  
  
\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*