MADANAPALLEINSTITUTEOF TECHNOLOGY &SCIENCE

(UGC-AUTONOMOUS INSTITUTION)
Affiliated to JNTUA, Ananthapuramu &Approved by AICTE, New Delhi
NAAC Accredited with A+ Grade,
NBA Accredited -B.Tech. (CIVIL, CSE, ECE, EEE, MECH), MBA & MCA

DEARTMENT OF COMPUTER SCIENCE & ENGINEERING-DATA SCIENCE

Assignment Submission Details

AY-2024- 25

Subject: SOC- Skill Oriented Course – V

Subject Code: 20CSD609

Subject Name: CRYPTOGRAPHY ALGORITHMS

Name of the Student	**S Raju**
Roll. No.	**22695A3208**
Year /Sec	**IV – CSE (DS)-B Sec**
Assignment No.	**I // II**
Marks (**Max 5 Mark)	
Assignment Moodle uploaded Date	**Uploaded // Drafted - __________**
Faculty Sign with name & Date	

Q1 : Explain briefly about model for network security.

Q2: Explain about substitution and transposition techniques.

Q3: Write a Python program to encrypt and decrypt a message using AES algorithm.

Q1 : Explain briefly about model for network security.

1. Confidentiality (Data Encryption):

This is primarily concerning confidentiality about who could view some sensitive information. The cryptographic algorithms provide mechanisms to encrypt the data so that it is not seen by unauthorized entities.

Symmetric Encryption: It uses the same secret key for encryption and decryption. Some common algorithms are:

AES (Advanced Encryption Standard): It is very widely used for data protection due to the strength of the algorithm and its efficiency.

DES (Data Encryption Standard) and Triple DES: These are older methods of encryption, but they have already found their usage today in legacy systems where security can be compromised at any point of time.

2. Integrity (Data Integrity):

Cryptography functions ensure that the data in transit hasn't been modified.

Hash Functions: Functions which generates a fixed-size hash or digest from an arbitrary input, such that even a tiny change in an input yields a completely different hash.

SHA (Secure Hash Algorithm): Probably the most widely used family of cryptographic hash functions, including SHA-1, SHA-256 and SHA-3. SHA-256 is widely used in blockchain and digital certificates.

3. Authentication (Verifying Identity):

Authentication thus ensures the identity of who is communicating to whom is guaranteed.

Digital Certificates: Through public-key encryption, this binds a public key to an entity and verifies that a server or person is genuine. These certificates are signed by a trusted third-party CA.

4. Proof of Origin (Non-repudiation)

Non-repudiation prevents sender denial that indeed he is the sender of a message. It is an important feature in legal and commercial communications.

Digital Signature: It provides both authentication as well as non-repudiation. If there is any digital signature associated with the private key of the sender, then it is guaranteed that the sender cannot deny later that he was indeed the sender.

Audit Logs: In support of non-repudiation and using other cryptographic methodologies besides, logs that can be used to establish communications did indeed occur can be kept.

5. Key Management (Handling Cryptographic Keys Securely) :

Effective management of cryptographic keys is necessary for the proper working of the mechanisms for encryption and decryption.

Key Exchange Protocols: Diffie Hellman and Elliptic-curve Diffie-Hellman (ECDH) Algorithms provide two parties with a method of securely creating and sharing the secret key over an insecure channel, which can subsequently be used to encrypt the message symmetrically.

Public Key Infrastructure (PKI): This entails the use of digital certificates to handle the public keys. Thus PKI forms a framework through which it is possible to have a large-scale environment have safe communication.

6. Access Control (Restricting Network Access):

Cryptography algorithms support authentication and authorization mechanisms to be implemented in a secure manner in such a way that restrictions could be carried on access control-that is, only allowing some persons to have access to certain resources on a network.

Role-Based Access Control (RBAC): Access permission is granted to persons involved in an organization based on their respective role(s).

Multi-Factor Authentication (MFA): It employs more than one method, like passwords, biometrics, or one-time codes, to authenticate the users.

7. Threat Mitigation:

Encryption schemes also include protection against some network-specific threats like:

Man-in-the-Middle Attacks (MitM): The messages cannot be intercepted, nor modified by third parties due to the encryption and digital signature.

Replay Attack: Use of time-stamps as well as nonces, a random number used once, prevents the malicious replay of previous messages.

8. VPNs and TLS/SSL:

VPNs: Use encryption protocols such as IPsec or SSL/TLS to develop secure channels of information over insecure networks.

TLS/SSL: It secures the communication between the web browsers and the servers by encrypting the HTTP traffic. Thus, all communication between browser and server is done as HTTPS. TLS/SSL uses both symmetric and asymmetric encryption for the security.

9. Quantum-Resistant Cryptography:

Most of the present cryptographic algorithms are based on RSA and ECC and are susceptible to quantum attacks, following the advent of quantum computing. There is a category of research called post-quantum cryptography with a focus of designing algorithms that can be proved resistant to the quantum computers' computational power, such as Lattice-based cryptography.

Q2: Explain about substitution and transposition techniques.

The two techniques in classical cryptography by which plaintext is being obscured to ensure proper security of the message being transmitted are substitution and transposition. Here's a short overview for each of them.

Substitution Techniques:
Substitution is a method in which every letter or symbol of the plaintext is replaced by some other letter, symbol, or even number. The principle of substitution is the systematic substitution of characters to form the ciphertext.

Caesar Cipher: This is one of the simplest forms of a substitution cipher. Each letter in the plaintext is shifted along the alphabet by a fixed number of positions. For example, a shift of 3 means that "A" becomes "D," "B" becomes "E," and so on.

Monoalphabetic Cipher Replace each letter of the plaintext by another letter or symbol according to some fixed mapping. That is, any random substitution can be used, but it is not true for the Caesar cipher, where the shift is uniform.

Poly-Alphabetic Cipher: This cipher employs several substitution alphabets that make it impossible to analyze the frequency of the encrypted text. No doubt that the most popular example of poly-alphabetic cipher is the Vigenère Cipher. It relies on a key to determine which shift should be used with each letter, which in turn makes the deciphering harder than it would have been with mono-alphabetic ciphers.
Advantages:
Poly-alphabetic ciphers are much safer than plain mono-alphabetic ciphers by spreading the letter frequencies.
Disadvantages:

Monoalphabetic ciphers are vulnerable to frequency analysis because letters that appear most frequently in a language-text like "E" is known for the English language-will be easily identified and cracked.
Transposition Techniques
Transposition techniques merely re-arrange the characters in the plaintext without altering the characters themselves.

Rail Fence Cipher: Letters of the plaintext are written in a zigzag pattern across multiple rows, then read off row by row to form the ciphertext. For instance, "HELLO" could be encoded as "HLOEL" using two rows.

Columnar Transposition Cipher: The plaintext is arranged in a grid or matrix and then transposed according to the columns with a key. For instance, if the key is "KEY", the columns are rearranged according to the alphabetical order of the key.

Double Transposition Cipher: This is a complex procedure involving double rounds of transposition, where often two different keys are used for the two rounds. This makes the cipher much more difficult to break.

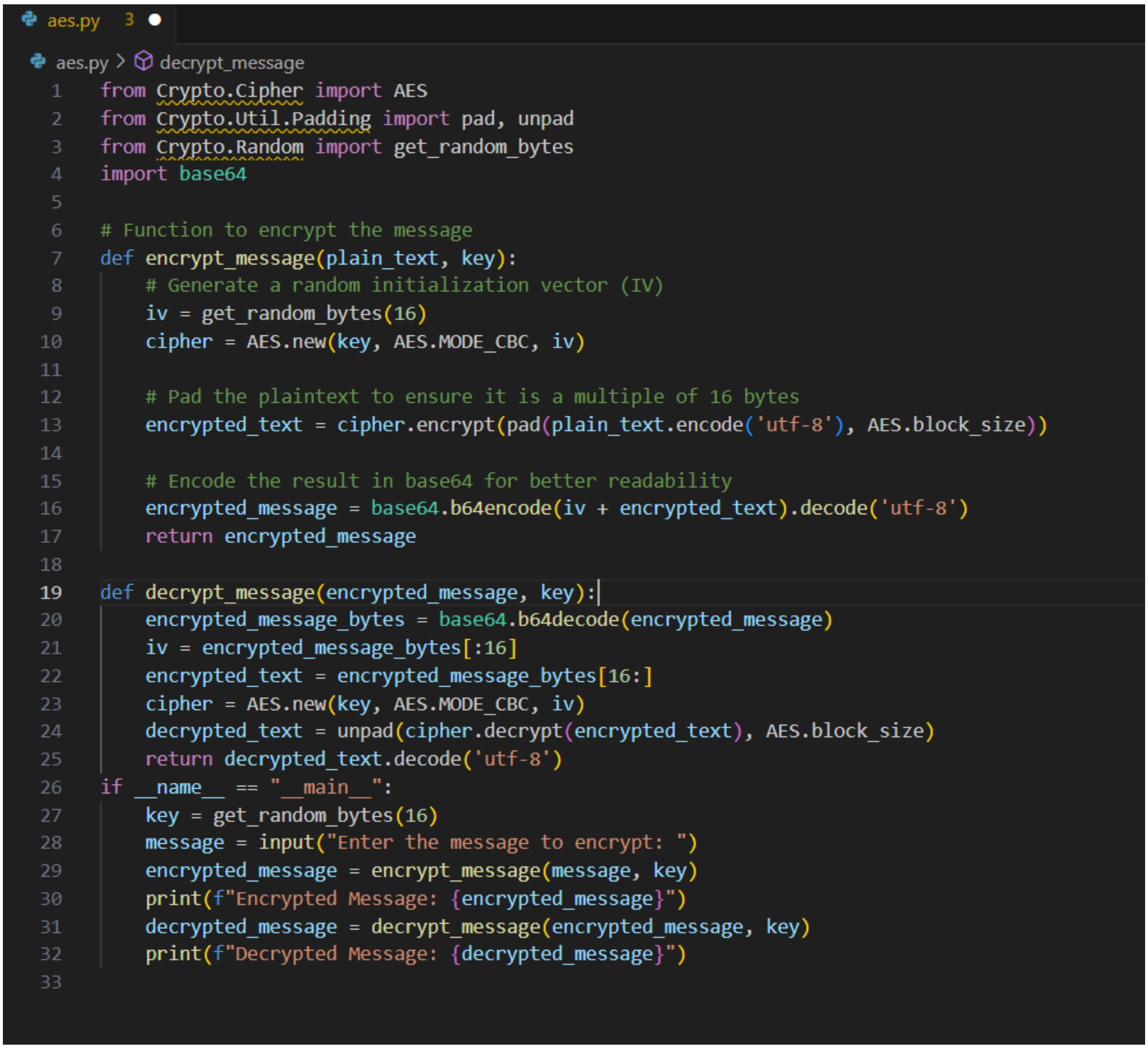
Strengths:

Transposition ciphers do not change character frequencies thus are more difficult to crack by simple analysis.

Weaknesses:

If the transposition pattern or key is known, one can easily reconstruct the original message.
Comparison:
Substitution replaces characters while transposition reorder them.
Letter frequencies are affected in substitution while it does not change the frequency distribution in transposition.

Q3: Write a Python program to encrypt and decrypt a message using AES algorithm.



```python
from Crypto.Cipher import AES
from Crypto.Util.Padding import pad, unpad
from Crypto.Random import get_random_bytes
import base64

# Function to encrypt the message
def encrypt_message(plain_text, key):
    # Generate a random initialization vector (IV)
    iv = get_random_bytes(16)
    cipher = AES.new(key, AES.MODE_CBC, iv)

    # Pad the plaintext to ensure it is a multiple of 16 bytes
    encrypted_text = cipher.encrypt(pad(plain_text.encode('utf-8'), AES.block_size))

    # Encode the result in base64 for better readability
    encrypted_message = base64.b64encode(iv + encrypted_text).decode('utf-8')
    return encrypted_message

def decrypt_message(encrypted_message, key):
    encrypted_message_bytes = base64.b64decode(encrypted_message)
    iv = encrypted_message_bytes[:16]
    encrypted_text = encrypted_message_bytes[16:]
    cipher = AES.new(key, AES.MODE_CBC, iv)
    decrypted_text = unpad(cipher.decrypt(encrypted_text), AES.block_size)
    return decrypted_text.decode('utf-8')
if __name__ == "__main__":
    key = get_random_bytes(16)
    message = input("Enter the message to encrypt: ")
    encrypted_message = encrypt_message(message, key)
    print(f"Encrypted Message: {encrypted_message}")
    decrypted_message = decrypt_message(encrypted_message, key)
    print(f"Decrypted Message: {decrypted_message}")

```