Task T3

T3 Determine if the encryption scheme provides adequate security, and explain why.

The encryption scheme provides limited security:
Matrix Predictability:
The N x N matrices are smaller in size where N is 5 in this case and based on permutations, hence the matrices do not provide a high entropy level. Access to M1 and M2 matrices can lead to potential reverse engineering of the encryption pattern.
Deterministic Nature:
Each key and input pair lead to the same output, therefore repeated encryption with the same key will generate the same ciphertext which does not provide adequate security against brute force attacks.

The purpose of this study is to assess the asymmetric encryption scheme using permutation matrix lookups regarding the key principles of computer security, viz., confidentiality, integrity, and availability.

Analysis Security Adequacy

1. Confidentiality
Pros:
The use of random permutation matrices increases decryption time depending on the complexity of the permutation.
Cons:
Predictability; this scheme depends on the M1 matrix which maps the private key to the public key. Access to M1 could easily provide the option to reverse engineer the mapping between the public and private keys compromising confidentiality.
Vulnerable to plaintext attacks where if an attacker obtains several plaintext-ciphertext pairs can make the scheme vulnerable. Each plaintext value is mapped directly through matrix lookup rather than utilizing complex mathematical transformations like RSA hence with enough data an attacker can reconstruct the matrix values or predict encryptions.
The matrix lookup scheme lacks complexity making it vulnerable and easy to decrypt as the matrix is generated randomly within a fixed amount of N elements.

The scheme's dependency on matrix lookups rather than any complex mathematical transformations makes it susceptible to brute force, prediction, and reverse engineering compromising confidentiality.

2. Integrity

Pros:

Matrix lookup enforces a specified workflow for the decryption process, hence modification of data would lead to the difference between the decrypted output and the original plaintext.

Cons:

An attacker would be able to easily manipulate the matrix entries and alter the data since decryption would always provide a result without indication of any tampering. Decryption output could yield incorrect or random data without errors without the presence of any inherent detection system.

The scheme lacks integrity, an additional mechanism to detect tampering needs to be put in place to avoid data tampering.

3. Availability

Pros:

Matrix lookup is computationally simpler than complex mathematical operations leading to faster encryption and decryption processes, adding to availability.

Cons:

High dependency on Matrices can take a toll on availability if any of the matrices M1, M2, and M3 are incorrect leading to inaccurate decryption. Using a larger N adds to the consumption of computational memory and storage compromising availability.