Written Assignment 1

Q. Explain the padding scheme used in RSA. Why it is used? What is its limitation?

→ Padding schemes in RSA (Rivest-Shamir-Adleman) encryption are used to address certain vulnerabilities and limitations associated with the basic RSA algorithm. The most commonly used padding schemes in RSA are PKCS#1 v1.5 padding and OAEP (Optimal Asymmetric Encryption Padding). These padding schemes serve several important purposes:

1. Security: RSA encryption without padding can be vulnerable to attacks like the padding oracle attack, which can reveal information about the plaintext. Padding schemes add randomness and structure to the plaintext before encryption, making it harder for attackers to exploit vulnerabilities.

2. Data Integrity: Padding schemes ensure that the encrypted message can be decrypted correctly. They help distinguish between valid and invalid ciphertexts, preventing errors or tampering during transmission.

3. Preventing Attacks: Padding schemes prevent certain mathematical attacks on the RSA algorithm. Without padding, an attacker could potentially recover the plaintext by analyzing the ciphertext and exploiting patterns in the encryption process.

Two commonly used padding schemes in RSA:

1. PKCS#1 v1.5 Padding:

- PKCS#1 v1.5 padding is an older padding scheme used with RSA encryption.
- It involves adding a specific sequence of bytes to the plaintext before encryption.
- This padding includes a block type byte, random padding bytes, and a message digest.

- PKCS#1 v1.5 padding is still widely supported but is considered less secure than OAEP.

2. OAEP (Optimal Asymmetric Encryption Padding):

- OAEP is a more modern and secure padding scheme.
- It uses a hash function and a random number generator to add padding to the plaintext.
- OAEP padding is designed to provide better security against various cryptographic attacks, including chosen ciphertext attacks.
- It ensures that each encrypted message is unique, reducing the risk of patterns that could be exploited by attackers.

Limitations of Padding Schemes in RSA:

1. Padding Overhead: Padding schemes add additional bytes to the plaintext, increasing the size of the ciphertext. This can be a limitation when transmitting large amounts of data, as it may result in more significant overhead.

2. Compatibility: Different implementations of RSA may use different padding schemes. To decrypt a message, both the sender and receiver must use the same padding scheme. This can lead to compatibility issues when communicating with systems that use different padding schemes.

3. Security Vulnerabilities: While padding schemes enhance security, they are not immune to attacks. Vulnerabilities in the padding schemes themselves can be exploited by attackers. Therefore, it is crucial to use well-designed and secure padding schemes and keep them up to date.