Theory Assignment: 1

Name: Divya Shah; Branch: I.T (T.E.); Roll Number: 115 20/09/2023

Question: Explain the padding scheme used in RSA. Why it is used? What is its limitation? (LO mapped: LO2)

Solution:

- Introduction to RSA

RSA, which stands for Rivest-Shamir-Adleman, is a widely-used asymmetric encryption algorithm in cryptography. It involves the use of two keys, a public key for encryption and a private key for decryption. Padding schemes in RSA are used to ensure the security and reliability of the encryption process.

- Padding scheme in RSA

Padding in RSA is a crucial security measure. It involves adding random data to plaintext before encryption, ensuring ciphertext length varies for each message, thwarting attacks based on patterns. PKCS#1 v1.5 is common padding schemes. PKCS#1 v1.5 appends specific bytes for reliability and security. Padding mitigates vulnerabilities, but introduces overhead and necessitates proper implementation. However, it doesn't address all RSA security concerns, requiring consideration of other potential vulnerabilities.

$$RSA(m) = m^e mod\ N\ (for\ PKCS\#1\ v1.5)$$

Padding in RSA is the process of adding some random data to the plaintext before encryption. This is done for several reasons:

1. **Security**: Without padding, an attacker might be able to gain information about the plaintext based on the length of the ciphertext or the patterns in it. Padding ensures that each plaintext message has a unique ciphertext, making it more resistant to attacks.
2. **Reliability**: RSA encryption works with fixed-size blocks of data, and not all plaintexts will be the same size. Padding ensures that even variable-length plaintexts can be encrypted and decrypted correctly.
3. **Determinism**: Padding schemes help ensure that the encryption process is deterministic, meaning that the same plaintext will always produce the same ciphertext. This is important for reliable communication.

- Why is Padding Used:

Padding is used in RSA to enhance security by adding random data to plaintext before encryption, ensuring unique ciphertexts and safeguarding against attacks based on patterns.

- Limitation of Padding in RSA:

There are some limitations regarding padding in RSA which is mentioned below as follow:

1. **Padding Overhead:** Padding increases the size of the ciphertext, which can be a limitation in some applications, particularly when bandwidth or storage space is a concern.
2. **Padding Schemes Must Be Implemented Correctly:** If padding is not implemented correctly, it can introduce vulnerabilities that attackers could exploit. Proper implementation is crucial to the security of RSA.
3. **Padding Doesn't Solve All Security Issues:** While padding helps with certain security concerns, RSA is vulnerable to other attacks such as side-channel attacks and attacks that exploit vulnerabilities in the mathematical properties of RSA itself.
4. **Performance Overhead:** Some padding schemes, especially OAEP, can be computationally intensive, which can impact performance in resource-constrained environments.
5. Another limitation of RSA padding is its susceptibility to chosen-ciphertext attacks (CCA), where attackers can gain information about the plaintext by manipulating ciphertexts, potentially compromising security.