

Name: Harsh Hardasani

Batch: T12

Roll no: 35

## Assignment No. 4

**Aim:** Implementation and analysis of RSA cryptosystem and Digital Signature scheme using RSA.

### Theory:

#### PKCS

##### Algorithm: Encryption using PKCS#1v1.5

Input : Recipient's RSA public key  $(n, e)$ ;  $k = |n|$  bytes; Data 'D' of length  $|D|$  bytes with  $|D| \leq k-11$

Output : Encrypted data block of length  $k$  bytes.

1. Form the  $k$ -byte padded message block EB  
 $EB = 00 || 02 || PS || 00 || D$   
where  $||$  denotes concatenation and PS is a string of  $(k-|D|-3)$  non-zero randomly generated bytes(i.e., at least 8 random bytes)
2. Encrypt EB with the RSA Algorithm  
 $C = \text{RSA}(EB)$
3. Output C

### Output:

(19) WhatsApp

Virtual Labs

cse29-iiith.vlabs.ac.in/exp/pkcs/simulation.html

Public-Key Cryptosystems (PKCSv1.5)

★★★★☆

Rate Me

Report a Bug

Plaintext (string):

Saikarthik

encrypt

Ciphertext (hex):

2ebf94b241a4173d9fd8612d8e78c8ad03322da845bceffbdadd61e11f21cb  
bf8061fae2f6174d97008cedd4d4f5fe20da97aac6b7d7421463b6e3a7bc21ba  
424486eafdb589a7415299dd42f0a5cb0940ca28b65c622027201431ff6fba31  
4d20126891244048a5ee41581499ede09d64effa0800c60168ce24af2069706e

decrypt

Decrypted Plaintext (string):

Saikarthik

Status:

Decryption Time: 21ms

RSA private key

1024 bit 1024 bit (e=3) 512 bit 512 bit (e=3) Generate bits = 512

Modulus (hex):

a5261939975948bb7a58dffe5ff54e65f0496f9175f5a09288810b0975871e99  
af3b5dd94057b0fc07535f5f97444504fa35169d461d0d30cf0192e307727c06

**Conclusion:** In conclusion, the implementation and analysis of the RSA cryptosystem and Digital Signature scheme using RSA demonstrate the effectiveness of RSA in providing both encryption and authentication. The RSA cryptosystem ensures secure data transmission through public-key encryption, while the Digital Signature scheme adds an additional layer of security by enabling message integrity and non-repudiation. The combination of these two mechanisms highlights RSA's strength in securing sensitive communications, although it requires careful key

management and computational resources due to the large prime numbers involved in key generation.

**LO Mapped:** LO2