PARSHVANATH CHARITABLE TRUST'S

A. P. SHAH INSTITUTE OF TECHNOLOGY

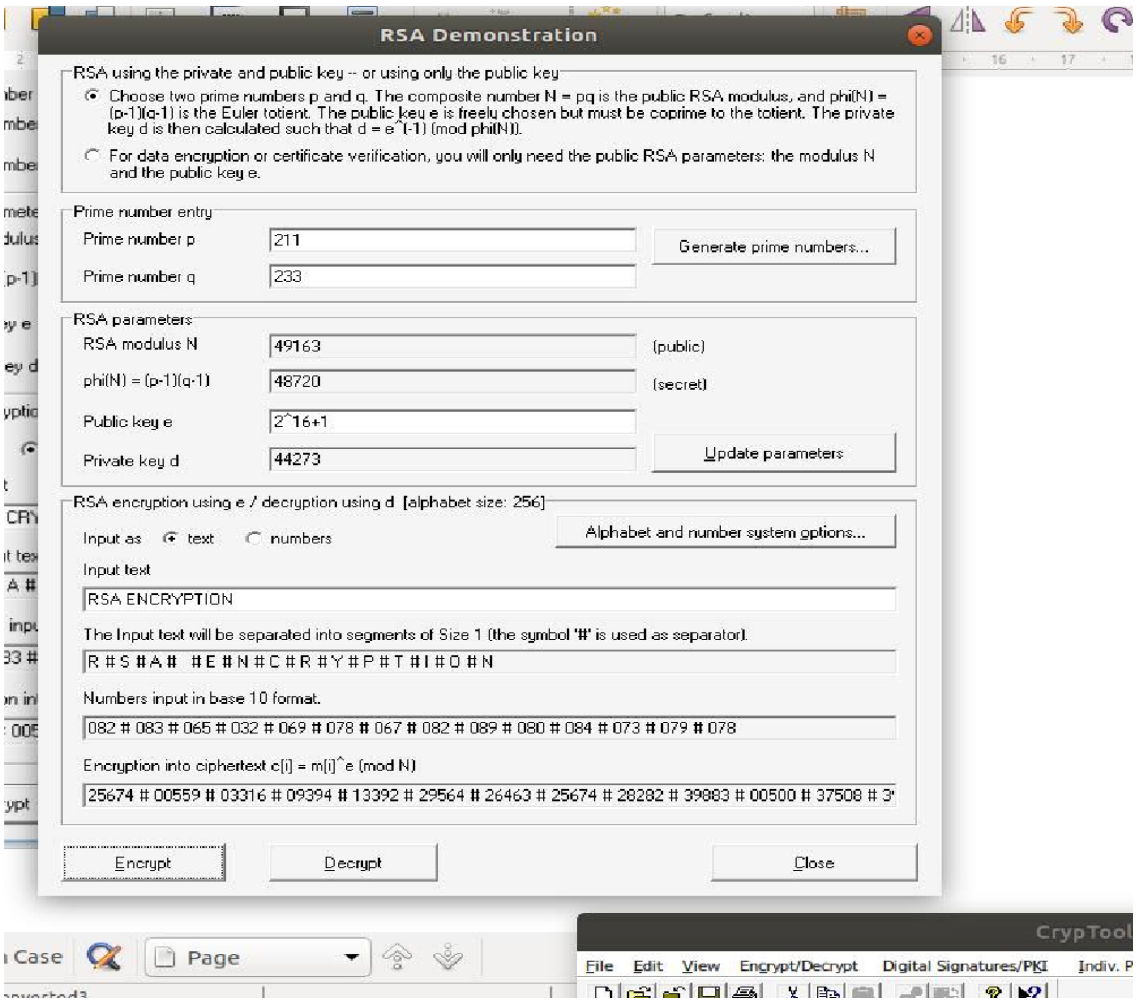
Department of Information Technology

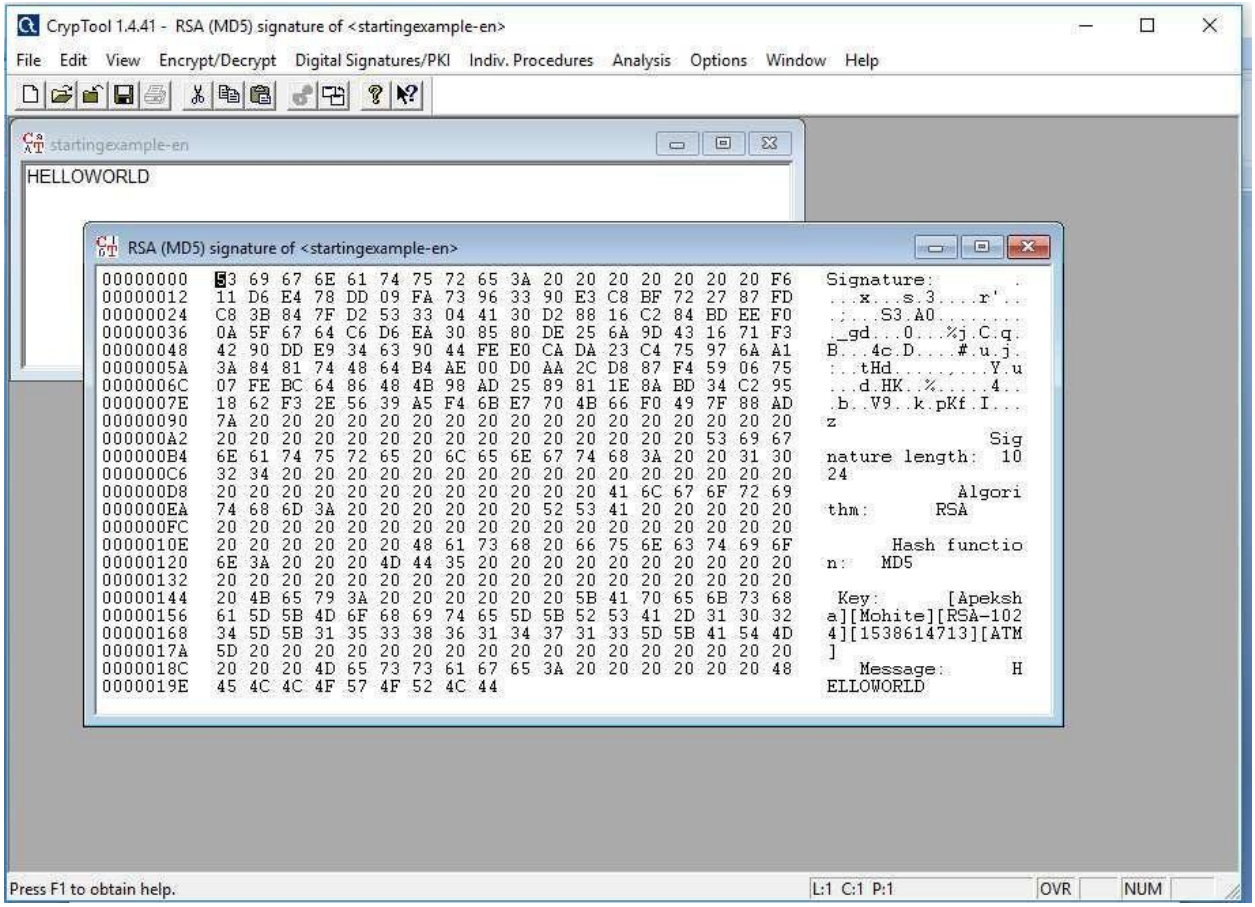
(NBA Accredited)

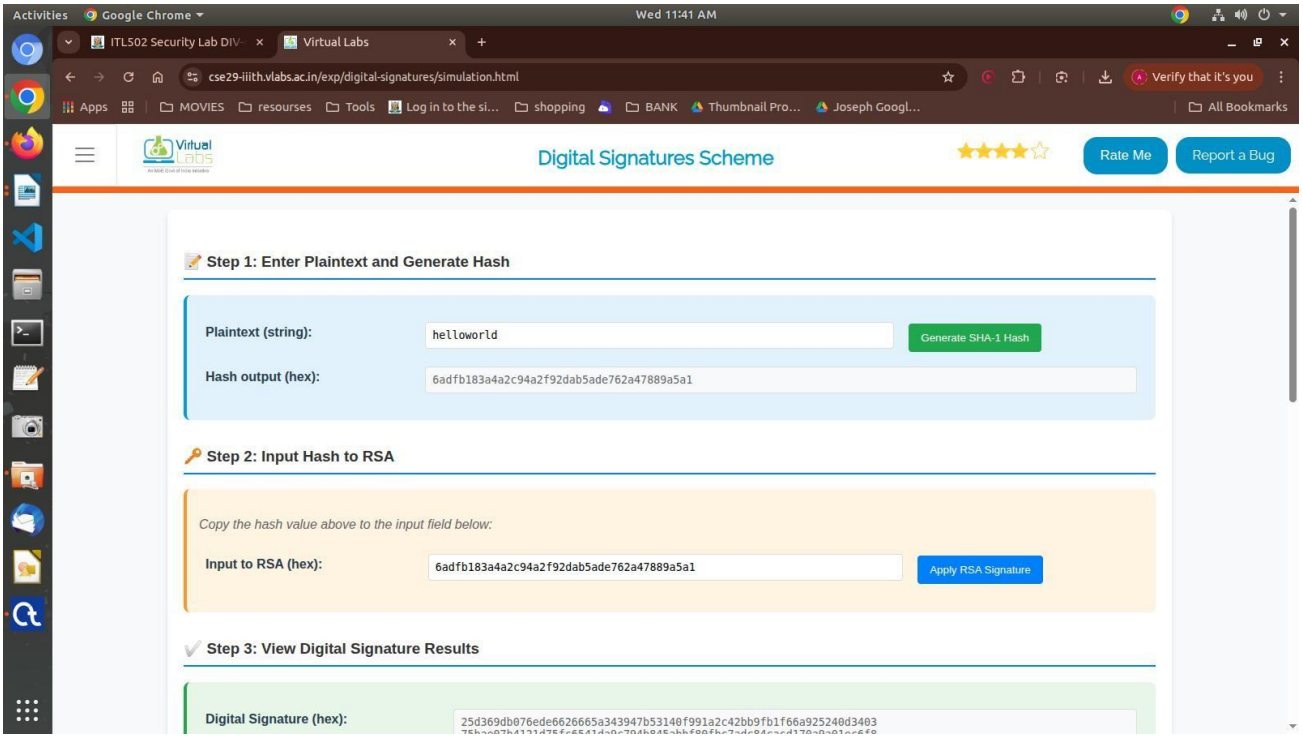
Academic Year: 2025-2026 **Semester: V**
Class / Branch: TE IT **Name of Student: Suyash Y Mane**
Subject: Security Lab
Subject In charge :Prof. Vishal Badgujar

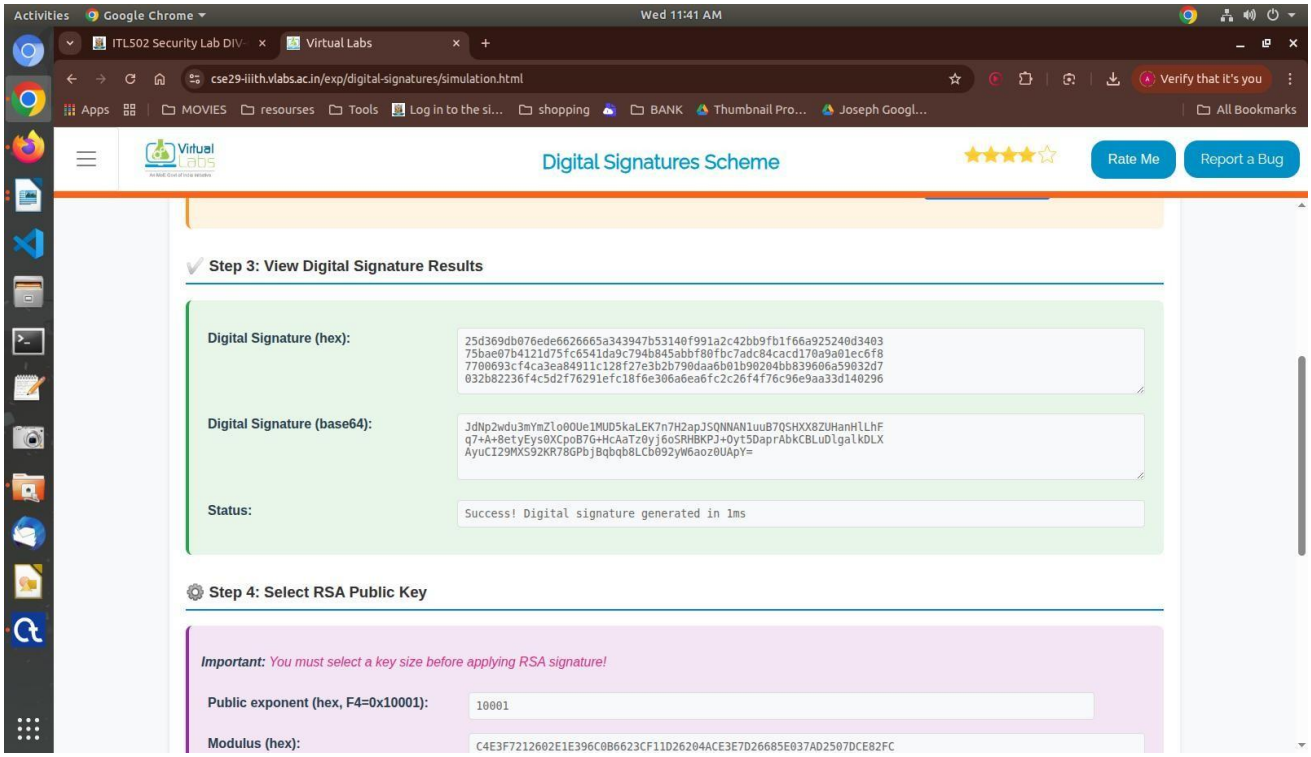
ExperimentNo.13(ii)

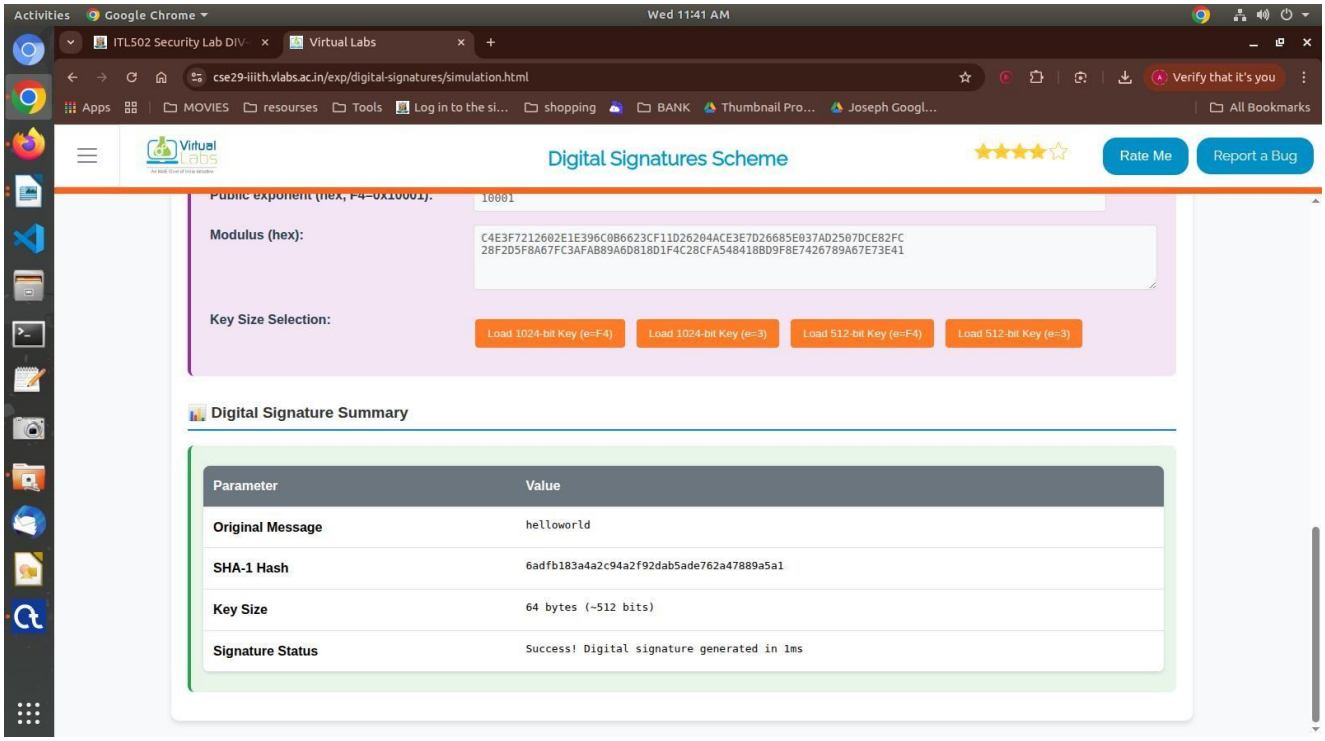
Aim: To study and analyze RSA crypto system and digital signature scheme.




CrypTool 1.4.41 - RSA (MD5) signature of <startingexample-en>
File Edit View Encrypt/Decrypt Digital Signatures/PKI Indiv. Procedures Analysis Options Window Help
startingexample-en
HELLOWORLD
RSA (MD5) signature of <startingexample-en>
00000000 53 69 67 6E 61 74 75 72 65 3A 20 20 20 20 20 20 F6 Signature: .
00000012 11 D6 E4 78 DD 09 FA 73 96 33 90 E3 C8 BF 72 27 87 FD ...x...s.3....r'..
00000024 C8 3B 84 7F D2 53 33 04 41 30 D2 88 16 C2 84 BD EE F0 .;...S3.A0.....
00000036 0A 5F 67 64 C6 D6 EA 30 85 80 DE 25 6A 9D 43 16 71 F3 ._gd...0...%j.C.q.
00000048 42 90 DD E9 34 63 90 44 FE E0 CA DA 23 C4 75 97 6A A1 B...4c.D....#.u.j.
0000005A 3A 84 81 74 48 64 B4 AE 00 D0 AA 2C D8 87 F4 59 06 75 :..tHd.....,...Y.u
0000006C 07 FE BC 64 86 48 4B 98 AD 25 89 81 1E 8A BD 34 C2 95 ...d.HK..%.....4..
0000007E 18 62 F3 2E 56 39 A5 F4 6B E7 70 4B 66 F0 49 7F 88 AD .b..V9..k.pKf.I...
00000090 7A 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 z
000000A2 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 53 69 67 Sig
000000B4 6E 61 74 75 72 65 20 6C 65 6E 67 74 68 3A 20 20 31 30 nature length: 10
000000C6 32 34 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 24
000000D8 20 20 20 20 20 20 20 20 20 20 20 20 41 6C 67 6F 72 69 Algori
000000EA 74 68 6D 3A 20 20 20 20 20 20 52 53 41 20 20 20 20 20 thm: RSA
000000FC 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
0000010E 20 20 20 20 20 20 48 61 73 68 20 66 75 6E 63 74 69 6F Hash functio
00000120 6E 3A 20 20 20 4D 44 35 20 20 20 20 20 20 20 20 20 20 n: MD5
00000132 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20
00000144 20 4B 65 79 3A 20 20 20 20 20 20 5B 41 70 65 6B 73 68 Key: [Apeksh
00000156 61 5D 5B 4D 6F 68 69 74 65 5D 5B 52 53 41 2D 31 30 32 a][Mohite][RSA-102
00000168 34 5D 5B 31 35 33 38 36 31 34 37 31 33 5D 5B 41 54 4D 4][1538614713][ATM
0000017A 5D 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20]
0000018C 20 20 20 4D 65 73 73 61 67 65 3A 20 20 20 20 20 20 48 Message: H
0000019E 45 4C 4C 4F 57 4F 52 4C 44 ELLOWORLD
Press F1 to obtain help.
L:1 C:1 P:1
OVR
NUM


Activities
Google Chrome
Wed 11:41 AM
ITL502 Security Lab DIV-
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/digital-signatures/simulation.html
Verify that it's you
Apps
MOVIES
resourses
Tools
Log in to the si...
shopping
BANK
Thumbnail Pro...
Joseph Googl...
All Bookmarks
Digital Signatures Scheme
Rate Me
Report a Bug
Step 1: Enter Plaintext and Generate Hash
Plaintext (string):
helloworld
Generate SHA-1 Hash
Hash output (hex):
6adfb183a4a2c94a2f92dab5ade762a47889a5a1
Step 2: Input Hash to RSA
Copy the hash value above to the input field below:
Input to RSA (hex):
6adfb183a4a2c94a2f92dab5ade762a47889a5a1
Apply RSA Signature
Step 3: View Digital Signature Results
Digital Signature (hex):
25d369db076ede6626665a343947b53140f991a2c42bb9fb1f66a925240d3403


Activities
Google Chrome
Wed 11:41 AM
ITL502 Security Lab DIV-
Virtual Labs
cse29-iiith.vlabs.ac.in/exp/digital-signatures/simulation.html
Verify that it's you
Apps
MOVIES
resourses
Tools
Log in to the si...
shopping
BANK
Thumbnail Pro...
Joseph Googl...
All Bookmarks
Digital Signatures Scheme
Rate Me
Report a Bug
Step 3: View Digital Signature Results
Digital Signature (hex):
25d369db076ede6626665a343947b53140f991a2c42bb9fb1f66a925240d3403
75bae07b4121d75fc6541da9c794b845abbf80fbc7adc84cacd170a9a01ec6f8
7700693cf4ca3ea84911c128f27e3b2b790daa6b01b90204bb839606a59032d7
032b82236f4c5d2f76291efc18f6e306a6ea6fc2c26f4f76c96e9aa33d140296
Digital Signature (base64):
JdNp2wdu3mYmZlo0OUe1MUD5kaLEK7n7H2apJSQNNAN1uuB7QSHXX8ZUHanHllhF
q7+A+8etyEys0XCpoB7G+HcAaTz0yj6oSRHBKPJ+Oyt5DaprAbkCBLuDlgalkDLX
AyuCI29MXS92KR78GPbjBqbqb8LCb092yW6aoz0UApY=
Status:
Success! Digital signature generated in 1ms
Step 4: Select RSA Public Key
Important: You must select a key size before applying RSA signature!
Public exponent (hex, F4=0x10001):
10001
Modulus (hex):
C4E3F7212602E1E396C0B6623CF11D26204ACE3E7D26685E037AD2507DCE82FC



Conclusion :

In this experiment. we learnt and understood how to study and analyze RSA crypto system and digital signature scheme.