Department of Information Technology

Semester: V
Academic Year: 2022-23
Class / Branch: TE IT
Subject: Security Lab (SL)
Name of Instructor: Prof. Apeksha Mohite

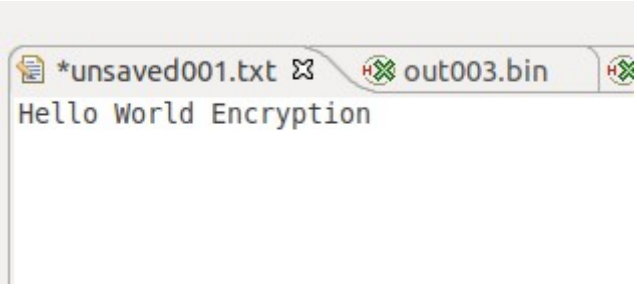
Name of Student: Vishal Bangar
Student ID: 20104084

EXPERIMENT NO. 12

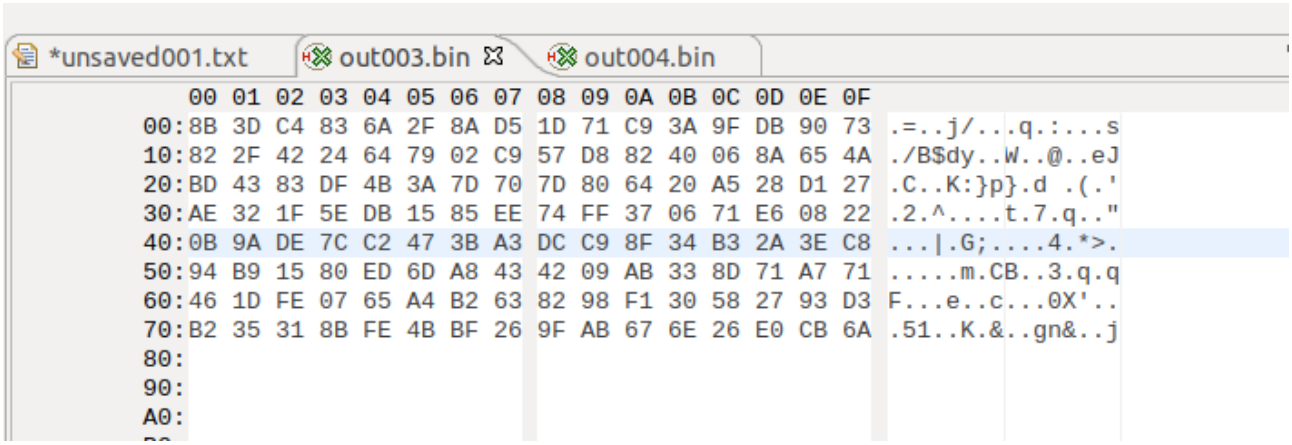
Aim: To study and analyze RSA cryptosystem and Digital Signature scheme

Output:

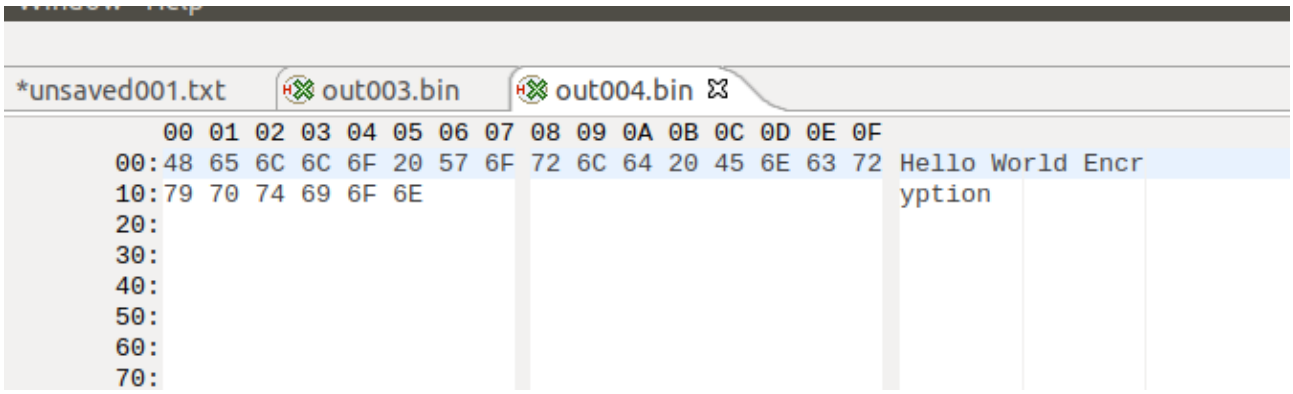
RSA



Encryption:


*unsaved001.txt
out003.bin
out004.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00:8B 3D C4 83 6A 2F 8A D5 1D 71 C9 3A 9F DB 90 73 .=..j/...q.:...s
10:82 2F 42 24 64 79 02 C9 57 D8 82 40 06 8A 65 4A ./B$dy..W..@..eJ
20:BD 43 83 DF 4B 3A 7D 70 7D 80 64 20 A5 28 D1 27 .C..K:}p}.d .(.'
30:AE 32 1F 5E DB 15 85 EE 74 FF 37 06 71 E6 08 22 .2.^....t.7.q.."
40:0B 9A DE 7C C2 47 3B A3 DC C9 8F 34 B3 2A 3E C8 ...|.G;....4.*>.
50:94 B9 15 80 ED 6D A8 43 42 09 AB 33 8D 71 A7 71 .....m.CB..3.q.q
60:46 1D FE 07 65 A4 B2 63 82 98 F1 30 58 27 93 D3 F...e..c...0X'..
70:B2 35 31 8B FE 4B BF 26 9F AB 67 6E 26 E0 CB 6A .51..K.&..gn&..j
80:
90:
A0:

Decryption:


*unsaved001.txt
out003.bin
out004.bin
00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00:48 65 6C 6C 6F 20 57 6F 72 6C 64 20 45 6E 63 72 Hello World Encr
10:79 70 74 69 6F 6E yption
20:
30:
40:
50:
60:
70:

Generate Key Pair