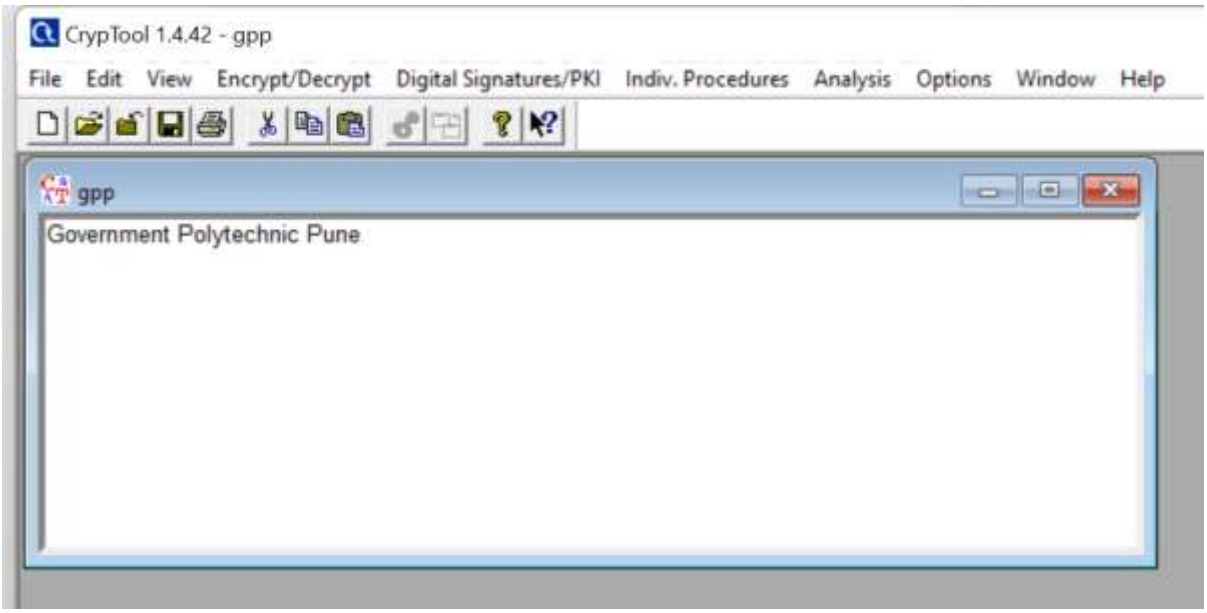
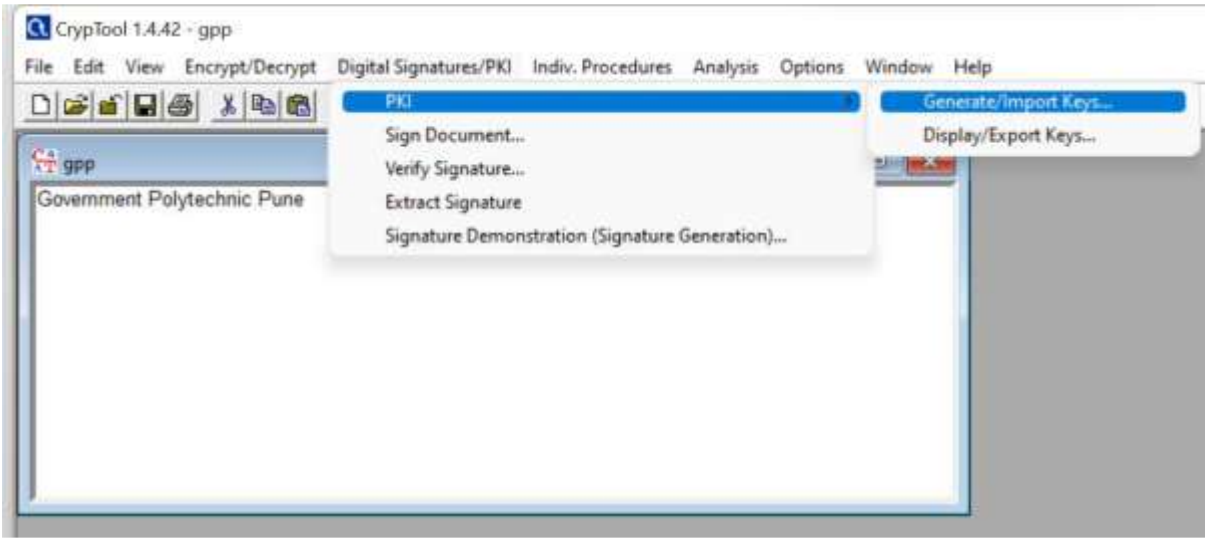
Practical No: - 8

Steps: -

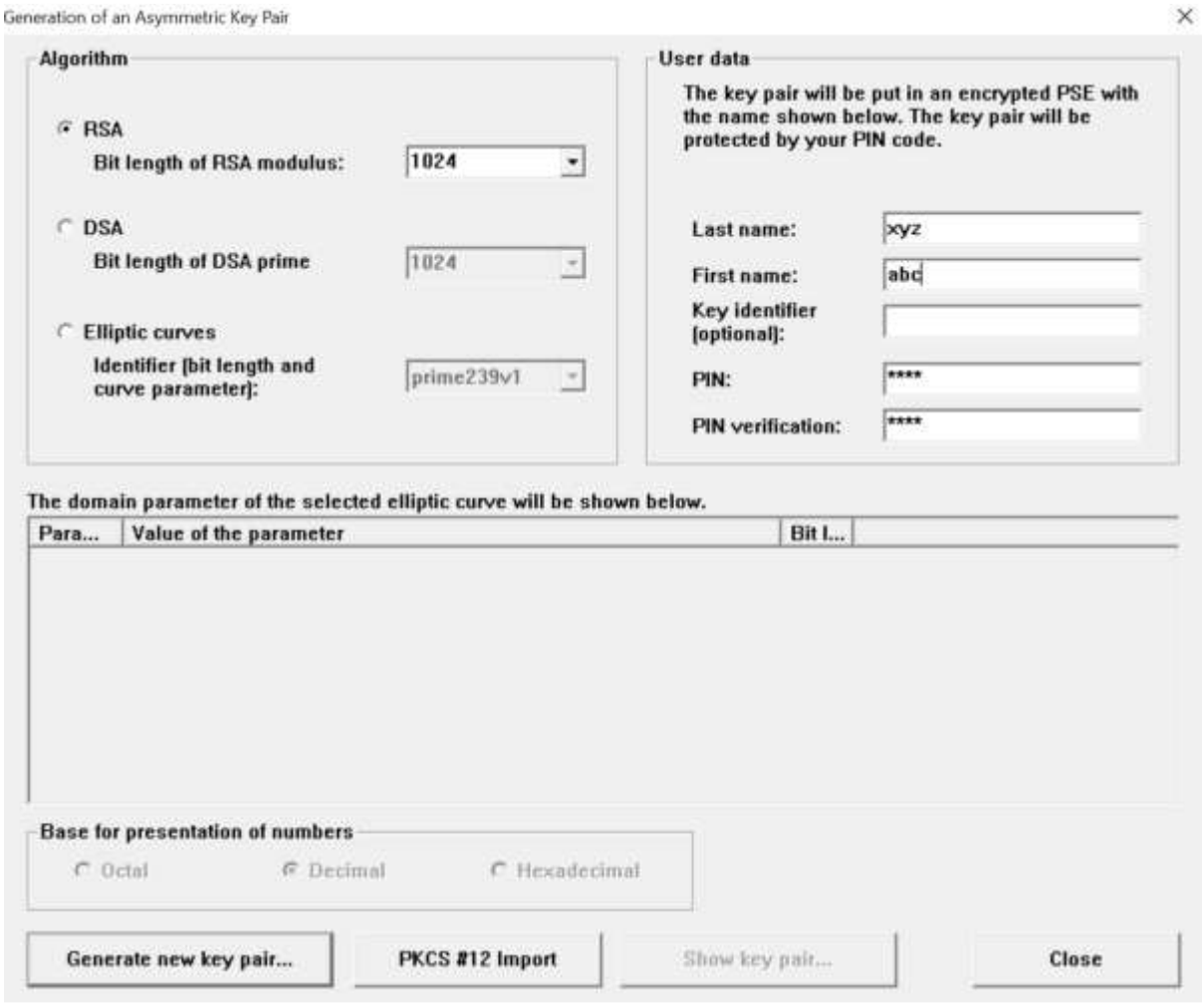
1. Go to cryptool software and create new file with some contents as shown below.



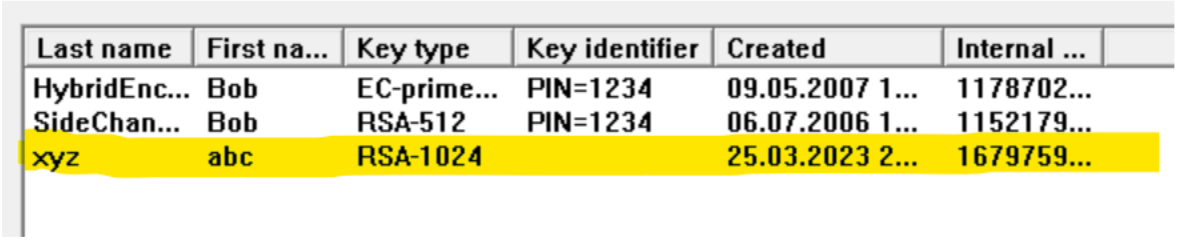
2. Now click on Digital signatures/PKI and then select PKI after that click on generate/import keys.



3. And then select RSA algorithm, fill required user data and then click on generate new key pair.

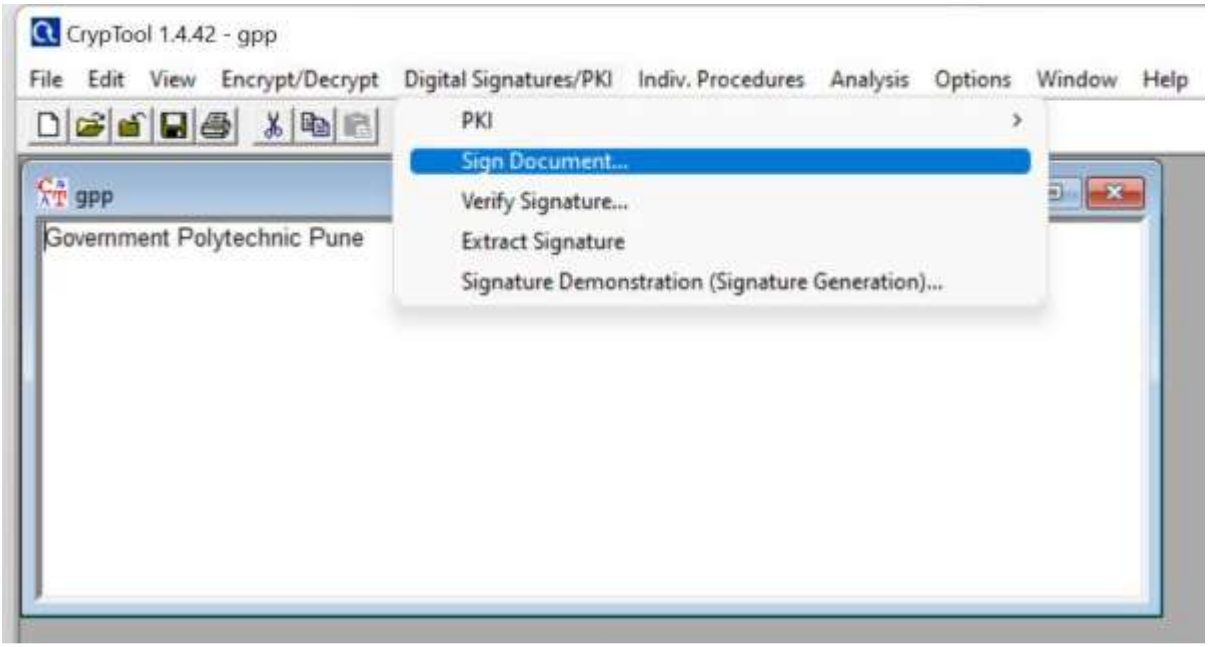


4. Now click on show key pair to see generated key.

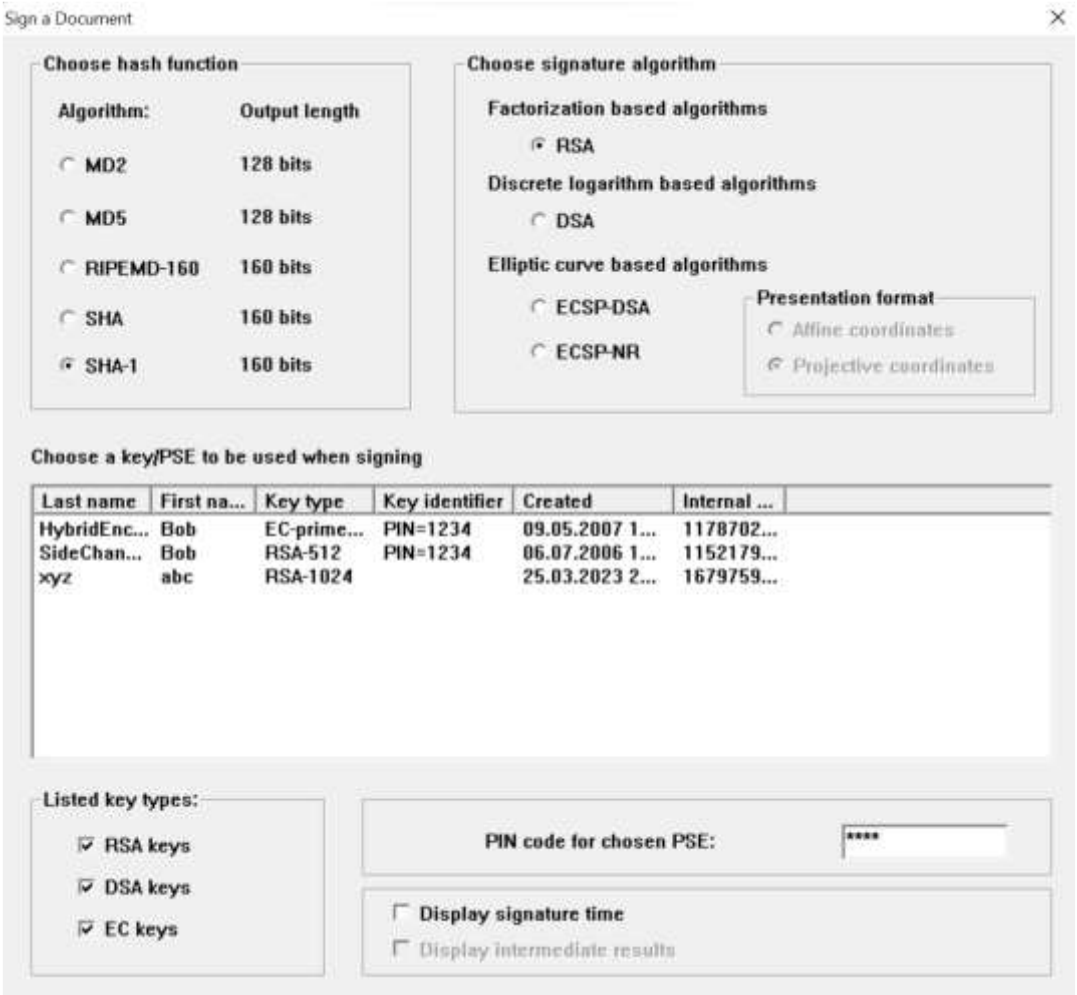


Last name	First na...	Key type	Key identifier	Created	Internal ...
HybridEnc...	Bob	EC-prime...	PIN=1234	09.05.2007 1...	1178702...
SideChan...	Bob	RSA-512	PIN=1234	06.07.2006 1...	1152179...
xyz	abc	RSA-1024		25.03.2023 2...	1679759...

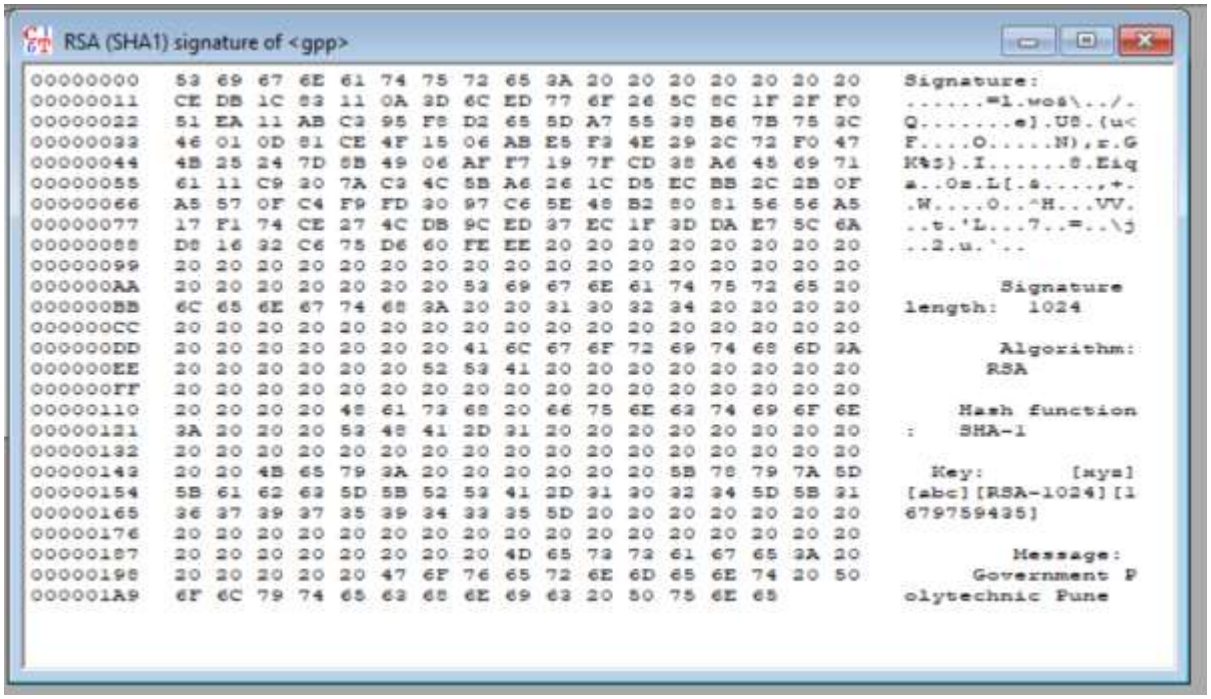
5. Now again go to Digital Signatures/PKI and click on Sign Document



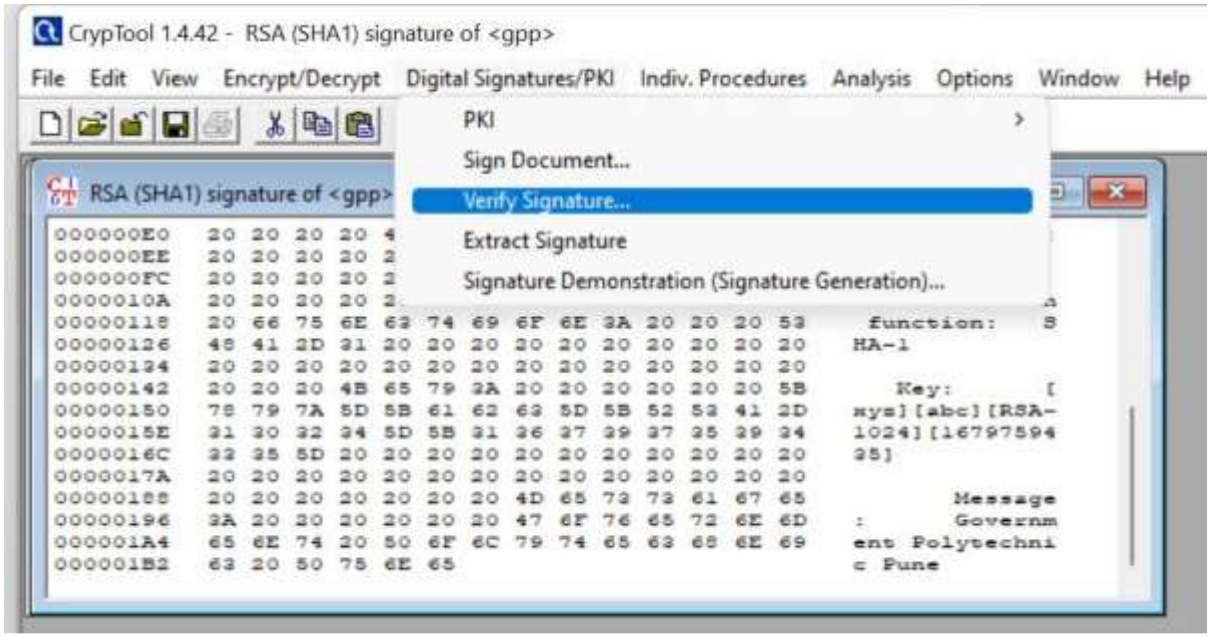
6. After that select our generated key & enter pin then click on sign.



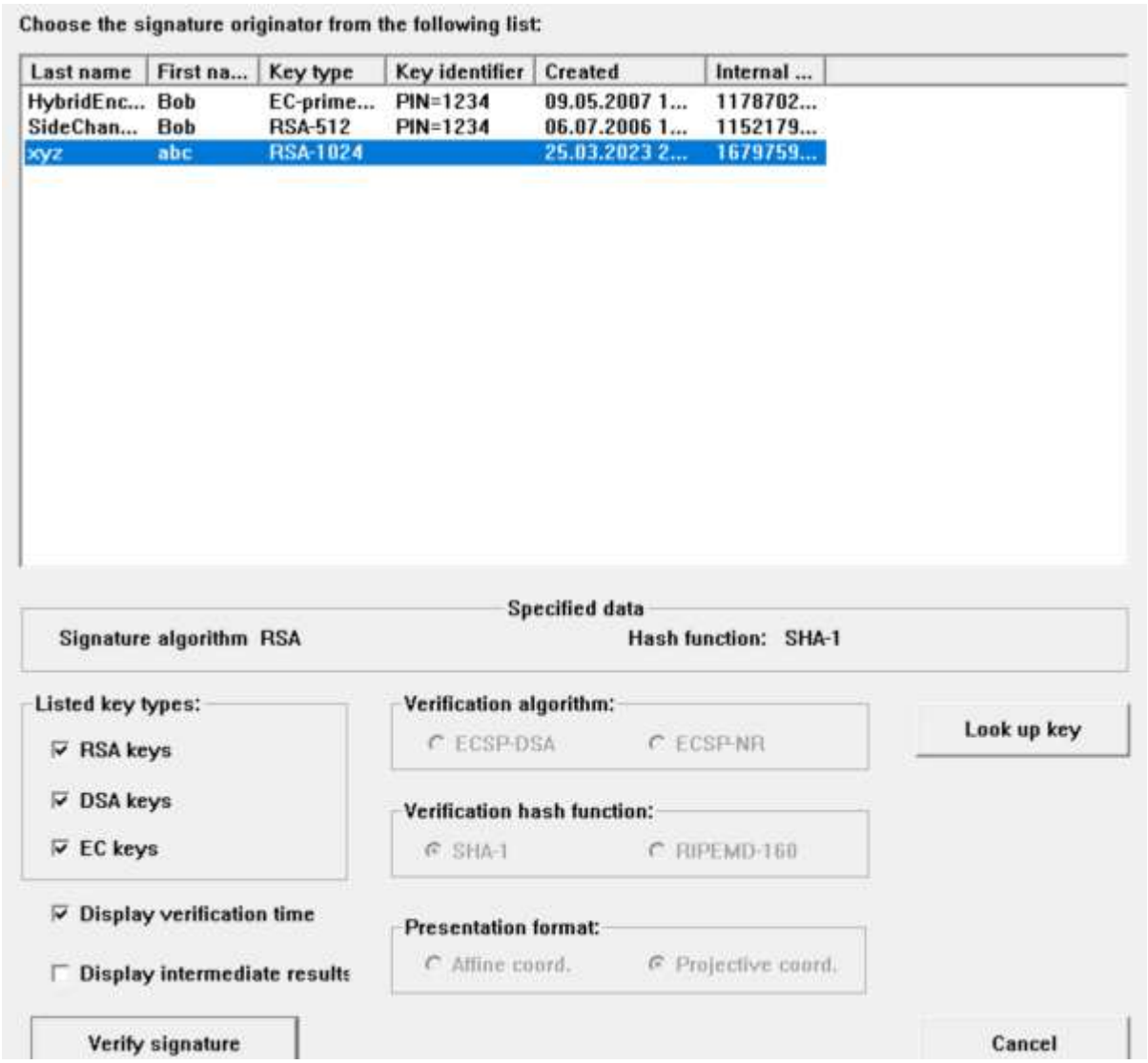
7. After clicking on sign option this will gives the following signature



8. Now again go to Digital Signatures/PKI and click on Verify Signature



9. Then select our generated key and click on Verify Signature.



10. After clicking on Verify Signature, this will give following message if the correct.