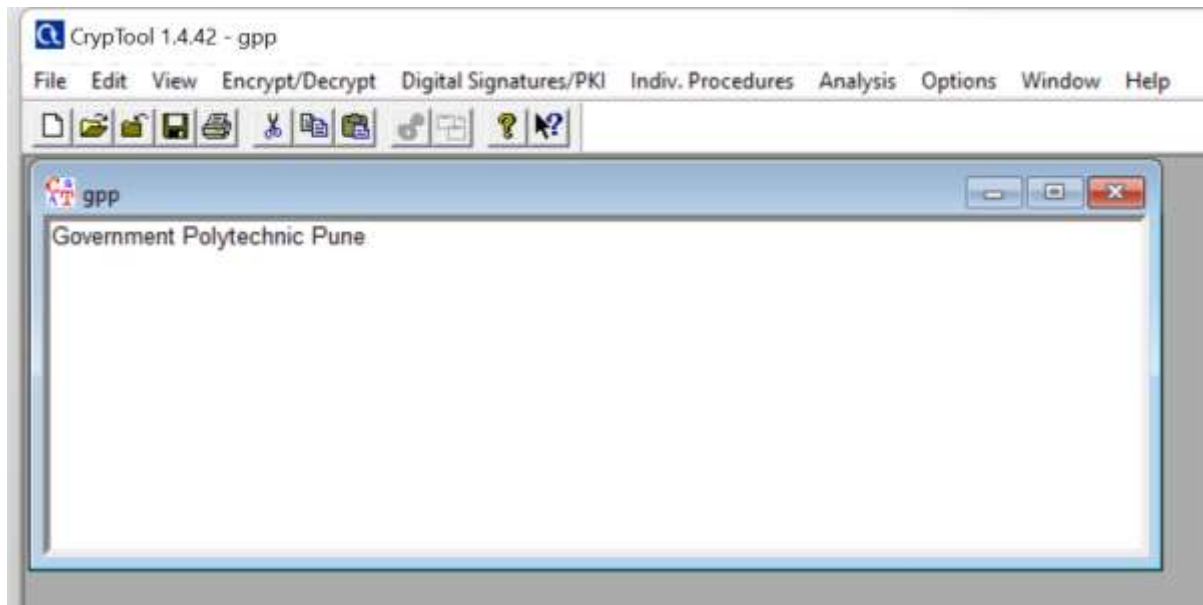


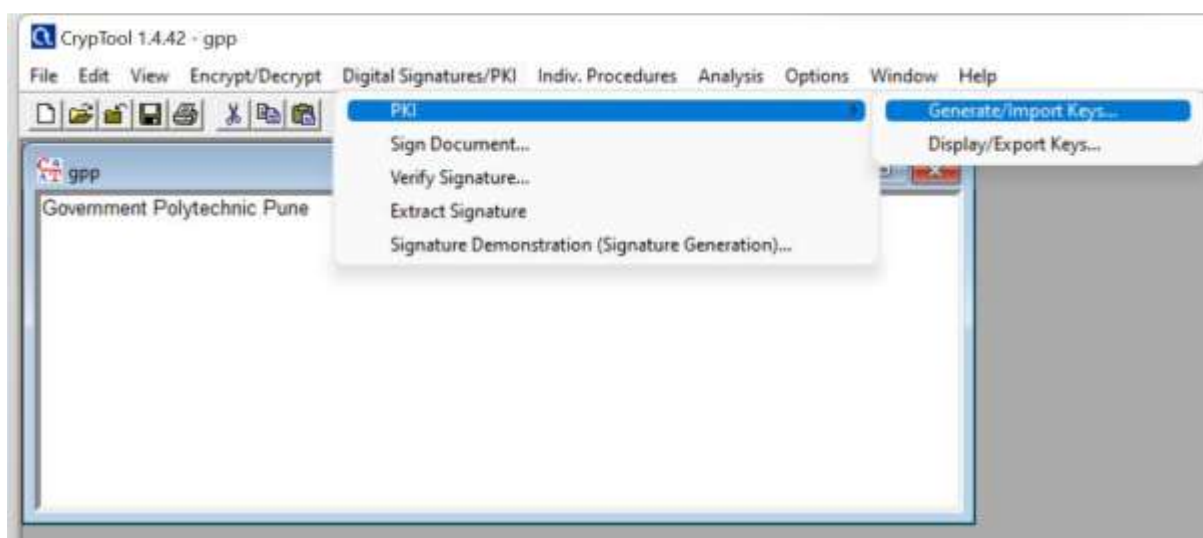
## Practical No: - 8

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.



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

Generation of an Asymmetric Key Pair

**Algorithm**

☒ RSA  
Bit length of RSA modulus: 1024

☐ DSA  
Bit length of DSA prime: 1024

☐ Elliptic curves  
Identifier (bit length and curve parameter): prime239v1

**User data**

The key pair will be put in an encrypted PSE with the name shown below. The key pair will be protected by your PIN code.

Last name: xyz

First name: abc

Key identifier [optional]:

PIN: \*\*\*\*

PIN verification: \*\*\*\*

The domain parameter of the selected elliptic curve will be shown below.

Para...	Value of the parameter	Bit l...

**Base for presentation of numbers**

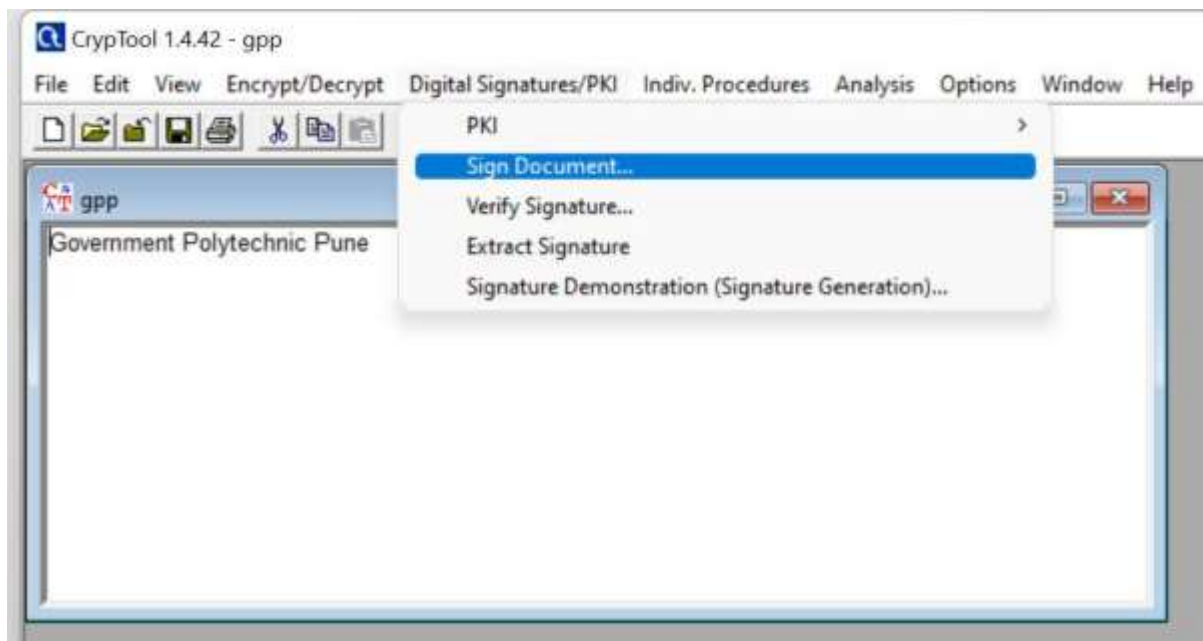
☐ Octal ☒ Decimal ☐ Hexadecimal

Generate new key pair... PKCS #12 Import Show key pair... Close

- 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...

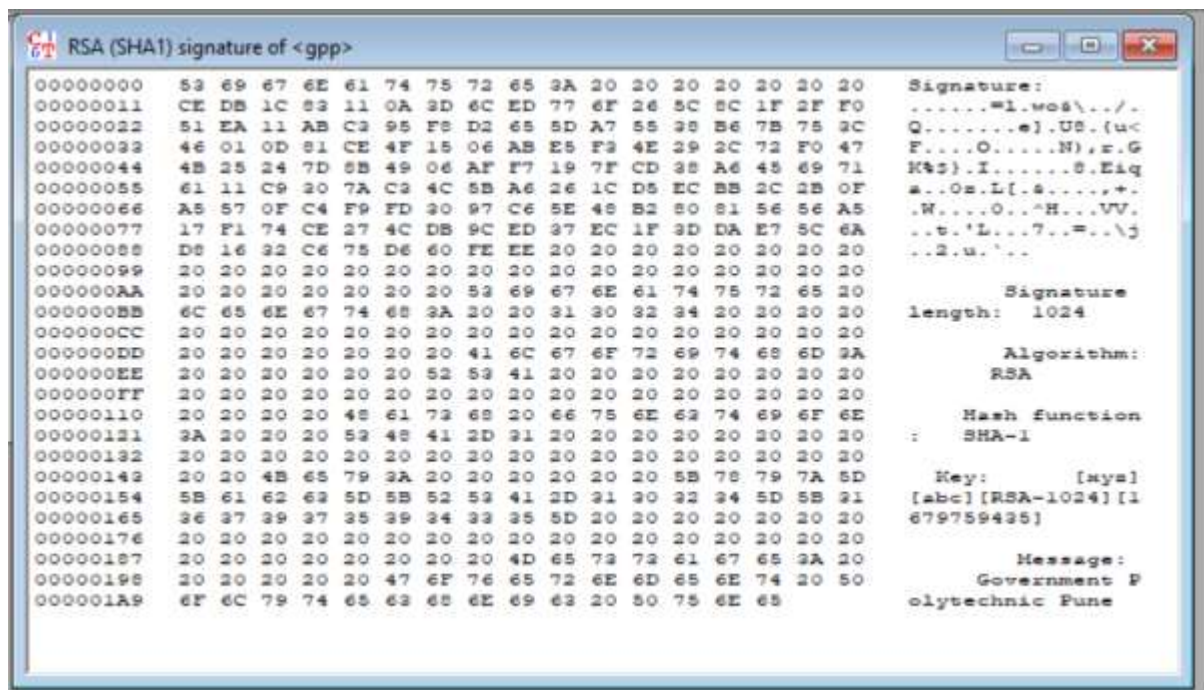
5. Now again go to Digital Signatures/PKI and click on Sign Document



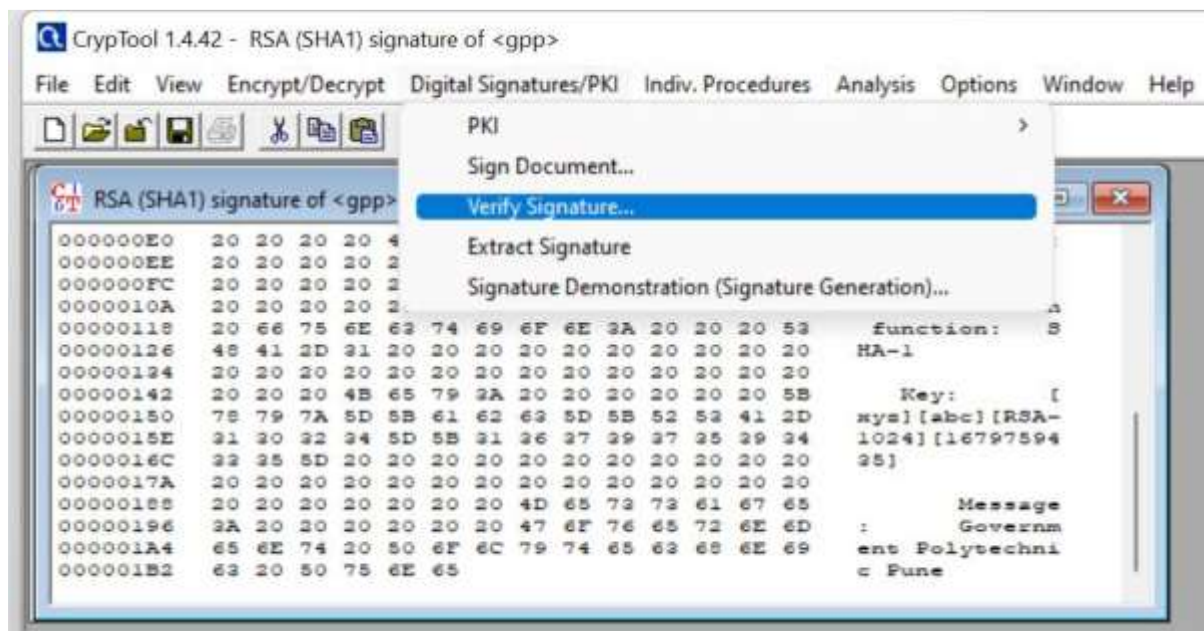
6. After that select our generated key & enter pin then click on sign.



7. After clicking on sign option this will give 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.

Choose the signature originator from the following list:

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...

Specified data

Signature algorithm: RSA Hash function: SHA-1

Listed key types:

- ☒ RSA keys
- ☒ DSA keys
- ☒ EC keys

☒ Display verification time  
☐ Display intermediate results

Verification algorithm:

- ☐ ECSP-DSA
- ☐ ECSP-NR

Look up key

Verification hash function:

- ☒ SHA-1
- ☐ RIPEMD-160

Presentation format:

- ☐ Affine coord.
- ☒ Projective coord.

Verify signature Cancel

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

CrypTool



Correct signature!

Duration of signature verification: 0.000 seconds.

OK