**Week-10** **Date: 15/04/2023**

**Demonstrate how to provide secure data storage, secure data transmission and for creating digital signatures (GnuPG)**

Open Terminal in Ubuntu and enter the following commands:

1. **sudo apt-get install update** //install and update all libraries
2. **sudo apt-get install gnupg** //install gnupg
3. **sudo apt autoremove** //autoremove
4. **gpg --gen-key** //generate gpg key

**Terminal Output**

Real name: Veeranna
Email address: 20r11a6607@gcet.edu.in

You selected this USER-ID:
"veeranna <20r11a6607@gcet.edu.in>"

Change (N)ame, (E)mail, or (O)kay/(Q)uit? O

gpg: key CD1991B894A3162C marked as ultimately trusted
gpg: revocation certificate stored as '/home/gcet/.gnupg/openpgp-revocs.d/D38A3435BAE5740C1DD3D4DACD1991B894A3162C.rev'
public and secret key created and signed.

pub rsa3072 2023-04-15 [SC] [expires: 2025-04-14]
D38A3435BAE5740C1DD3D4DACD1991B894A3162C
uid veeranna 20r11a6607@gcet.edu.in
sub rsa3072 2023-04-15 [E] [expires: 2025-04-14]

5. **gpg --output revoke.asc --gen-revoke Veeranna** //revoking process

**Terminal Output**

sec rsa3072/CD1991B894A3162C 2023-04-15 veeranna 20r11a6607@gcet.edu.in

Create a revocation certificate for this key? (y/N) y
Please select the reason for the revocation:
0 = No reason specified
1 = Key has been compromised
2 = Key is superseded
3 = Key is no longer used
Q = Cancel
(Probably you want to select 1 here)

Your decision? 0
Enter an optional description; end it with an empty line:
> testing
>
Reason for revocation: No reason specified
testing

Is this okay? (y/N) y
ASCII armored output forced.
File 'revoke.asc' exists. Overwrite? (y/N) y
Revocation certificate created.

// Encrypting the data/file

6. **gpg --output doc.gpg --encrypt --recipient 20r11a6607@gcet.edu.in abc.txt**
7. **gedit doc.gpg** // viewing Encrypted file

**Output**

**Doc.gpg**

…ŒÈá4@9ÿc[_2¹Iîø+¶Yâx¦
‹Åa£ÖÊªgd€,-ïã©JIO×Â[•8´92Ç…ÊÛi²¥*G-
M|-õ-ä“EÃÉQ‡ì¼vÒj6ûtjÆÚcË%‘˜jþoÿC%ìS¶…î\…
Å'í$æ¾•-—=Š*ÚÒ¤nÑÆ²,s·ÚëC"«Ñ›’ë
2D%þïUì/æ·U2Š|ácž!^ÉùÙÂ•)X±>µàéá;àéM÷Pœ-Wï‰`Õ
ZÍ{ª-ô•v§ÆÓIõ·µ}ÔáÄr¼ú©óY
ú¾Fá\ø½De0ëW*r§%•2ñÙ^rz¡µUÞ2r“,%â
óþ'IÍï®í‡,‹÷;çDcÅ“lˆB¿™ä‘{
üÊŸ„×|å+°°zŽ&ûŽ$'-]LèyÎÉ]`ÛÎK_*oô
Aœñk© <A×CÎ
´ÙìIð †ïÛÑ5¹‡ø×ýL@AÙÔkÔªÑ¿0çè*f*l9
(ÒNJçŠ„•þSó:Èq‘:+j¶ŒŠ*f*G²žJõ¢ö©yÕ¬ŽØc>sNàïµmØ□<1’Cî|¿''/É=ÑŽ ¾ V(Íµ€

// Decrypting the file

8. **gpg --output aiml07.txt --decrypt doc.gpg**

gpg: encrypted with 3072-bit RSA key, ID 8DC8E1340B400939, created 2023-04-15
"veeranna <20r11a6607@gcet.edu.in>"

9. **ls aiml07.txt**
10. **gedit aiml07.txt** // Viewing the decrypted file

**Output**

/*
hello
*/

11. **gpg --output doc.sig --sign aiml07.txt** // Appling Digital Signature
12. **gedit doc.sig** // Viewing created digital signature

**Output**

**doc.sig**

£ãþnÛwR¢Ìæ‡¬b
aiml07.txtd:iÕ
/*
hello
*/
‰³ ! w½¯¼ ÉòÃ=qnÛwR¢Ìæ‡d:iÕ nÛwR¢Ìæ‡Ü
þ3äÖ(±÷¿°fCíxU'Æø.F ˜–*Yò¤FØ¤ª8”È{Û±ÅD¦0žõeŠÚ1Û°ƒÜLyô¨¬Õ®Öl€D¦
ÙJt†õüBµ_×–-r¯ ~`6dëE‹uO(L6Pƒxrh@ rIsRÿJ½wm‘õ-
0œÐ2ÃŸduéu›_¼Â{ÅÔ;X,œÞŒ£q,É-lÑ]_üÛ6¾5-¶Ä)ƒ-…bûM-
?æ$¤Òì{&1Îk˜-Æ¤ý©ªŽh‘nÌëÄ¨Z2M„18Š¥x||j«¥Y¨?Âei;
Š®8rñ™ëXçÕjÜcævIOvdáhWñl$!:´´8‹)¶‡˜%qê¾†“i¶MÿáLýV›ïz@xÌ
WÖÇÝàCÍtzN4,}§p#ËBÖc<•¦`+äMÐþÂR Á‰×üs’±¢á%,7u H²‹ ]jçb‹žó□B¬1–9k
¢TMŸ8~□›Së9?X[œ¯ö