**3. Creare un file di testo e cifrarlo con algoritmo AES256**

La passwd del file di testo è “jkm”

gpg -c –cipher-algo AES256 testo.txt

Questo comando serve per specificare il tipo di algoritmo, in questo caso AES256

gpg –symmetric testo.txt

Per default –symmetric usa AES256

<https://www.adamintech.com/how-to-encrypt-your-files-in-linux-by-using-gpg/>

**4. Verificate la presenza del file cifrato ed il suo contenuto con il comando “file”. Attenzione: il file originale non viene automaticamente rimosso**

Comando: file testo.txt.gpg

Output: testo.txt.gpg GPG symmetrically encrypted data (AES256 cipher)

**5. Verificate la non leggibilità del documento cifrato utilizzando un comando di visualizzazione (non un editor!)**

Comando: nano testo.txt.gpg

**6. Utilizzate un visualizzatore esadecimale per analizzare il contenuto del documento cifrato e verificare la presenza di caratteri non stampabili**

* Comando: xxd testo.txt.gpg
* Output:

00000000: 8c0d 0407 0302 3caf 33c1 6d00 edca ffd2 ......<.3.m.....

00000010: 4401 ccb6 69dc 28d3 36a4 1f27 2b9f bd5d D...i.(.6..'+..]

00000020: b102 c858 19c3 8a3b 8cd2 c4e6 0813 d73e ...X...;.......>

00000030: a401 6a7d f79a 4ce3 3078 84ac 5303 50ee ..j}..L.0x..S.P.

00000040: a657 1165 89a8 8c53 3c05 a9e2 f223 68f7 .W.e...S<....#h.

00000050: 2274 c97c e7 "t.|.

**7. Procedete a decrittare il file generato al punto 4 e verificate che il file di testo ottenuto sia identico a quello generato al punto 3 (di default l’output viene mandato sullo standard output, il video)**

Comando: gpg -d -o testo1.txt testo.txt.gpg

Verrà -o salva il contenuto del file criptato in un altro file

https://www.tecmint.com/gpg-encrypt-decrypt-files/

**8. E’ molto probabile che l’operazione del punto 7 non vi chieda di inserire la chiave (passphrase). Quale è la spiegazione di questo comportamento apparentemente strano? Come è possibile imporre che la passphrase venga richiesta?**

* La passphrase viene salvata nella cache, è per quello che non viene richiesta
* Per fare che la passphrase venga richiesta ogni volta che si vuole decriptare::

Comando: gpg --symmetric --no-symkey-cache testo.txt (per criptare)

<https://security.stackexchange.com/questions/103034/gnupg-decryption-not-asking-for-passphrase>

**9. Considerate nuovamente un file di testo in chiaro. La cifratura ottenuta precedentemente contiene caratteri non stampabili e renderebbe impossibile, per esempio, l’invio del file cifrato al destinatario tramite mail. Come è possibile cifrare il file in modo che contenga solo caratteri stampabili (codifica Base64)?**

* Comando: bas64 testo.txt > testo64.txt

**10. Decifrate il file cifrato del punto precedente in modo da riottenere il file di testo originale.**

* Comando: base64 --decode testo64.txt > testo646.txt