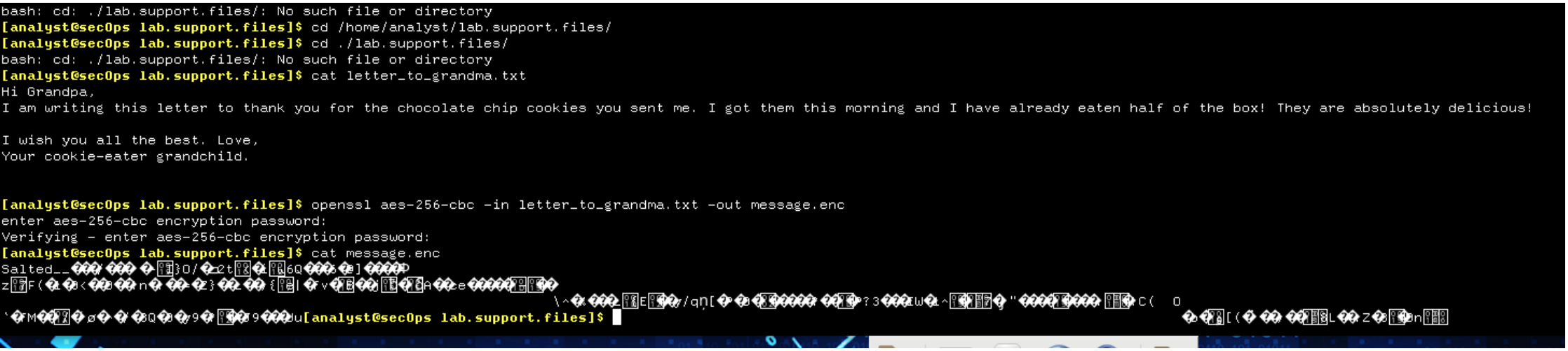
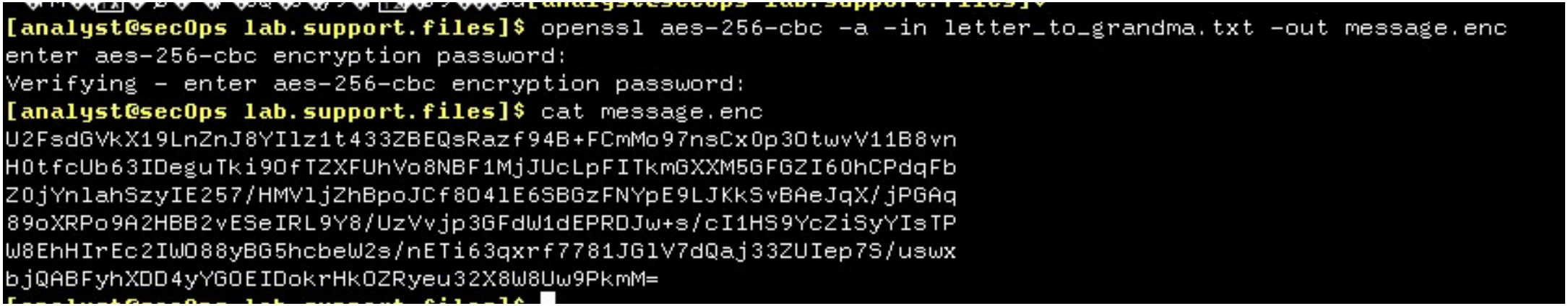
Partie 1 :



Nous avons crypté le message sous une autre clé de cryptage, ce pourquoi le texte est différent



Comme la clé a été modifié par un « -a », la clé change donc le résultat visible par cat.
Il est bien plus pratique d’utiliser une base64 car il est bien plus pratique d’utiliser des lettres et des chiffres pour décrypter des données (exemple en ASCII) que d’utiliser des « ? ».

Partie 2 :

```
[analyst@secOps lab.support.files]$ openssl aes-256-cbc -d -a -in message.enc -out lettre_dechiffree.txt
enter aes-256-cbc decryption password:
```

```
[analyst@secOps lab.support.files]$ cat decrypted_letter.txt
cat: decrypted_letter.txt: No such file or directory
[analyst@secOps lab.support.files]$ cat lettre_dechiffree.txt
Hi Grandpa,
I am writing this letter to thank you for the chocolate chip cookies you sent me. I got them this morning and I have already eaten half of the box! They are absolutely delicious!

I wish you all the best. Love,
Your cookie-eater grandchild.

[analyst@secOps lab.support.files]$
```

Terminal Emulator

c. Quand OpenSSL finit de déchiffrer le fichier **message.enc**, il enregistre le message déchiffré dans un fichier texte appelé **lettre_déchiffrée.txt**. Utilisez la commande **cat** pour afficher le contenu du fichier **lettre_déchiffrée.txt** :

`[analyst@secOps lab.support.files]$` **`cat decrypted_letter.txt`**

La lettre a-t-elle été correctement déchiffrée ?justifiez vos réponses ici

La commande utilisée pour déchiffrer contient également une option -a. Pouvez-vous expliquer pourquoi ?

cat decrypted_letter.txt ne marche pas, c'est logique puisque le fichier analysé n'existe pas. Celui qu'il faut utiliser est lettre-dechiffree.txt.

« Remarque : Base64 est un groupe de modèles de codage binaire vers texte semblables utilisés pour représenter des données binaires dans un format de chaîne ASCII. »
-a permet de modifier le cryptage en base64 tandis que sans -a, on aurait des « ? ».
-d permet de traduire le -a (la base64) en ASCII, transformant les données binaires en chaîne, nous rendant le texte de départ.