# Compte Rendue : TP CHIFFREMENTS SYMETRIQUE ET ASYMETRIQUE

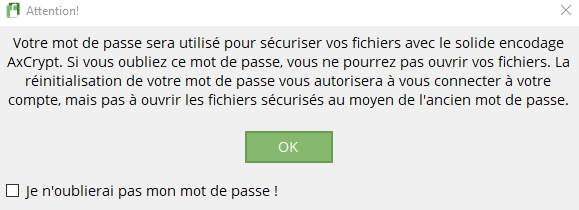
## Introduction :

Tout d’abord ce travail va nous faire utiliser un logiciel nommé AxCrypt, il va permettre le chiffrement symétrique. Le chiffrement symétrique est un système de chiffrement qui utilise la même clé secrète pour le chiffrement et le déchiffrement. C’est un chiffrement qui vous sera particulièrement utile pour chiffrer de grandes quantités de données. Ensuite nous avons utilisé ThunderBird qui va utiliser nos compte Gmail (crée juste pour ce travail). Cela va nous permettre de nous créer des clés personnelles et donc permettre le chiffrage de nos mails. Ce travail a pour but de nous faire découvrir de nouveau logiciel mais aussi d’apprendre a les utilisé pour de future travaux.

PARTIE 1 Chiffrement symétrique par fichier avec AxCrypt

## 1.1 Mise en place d’un logiciel de chiffrement de fichiers

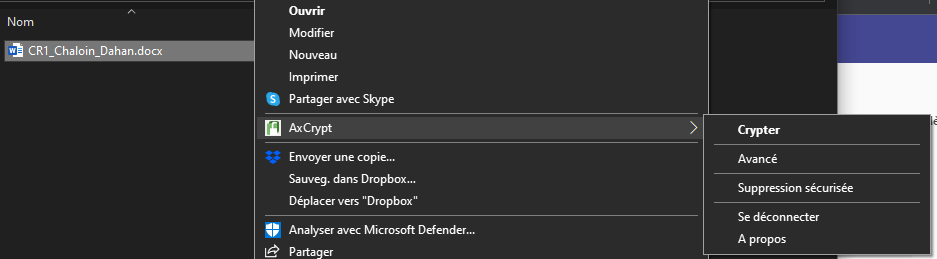
1°) Après avoir exécuté l’installeur et suivi les instructions, une fois le logiciel installé, il nous demandera de créer un compte avec une adresse mail et un mot de passe. Une fois les instructions suivies, ce message apparait :



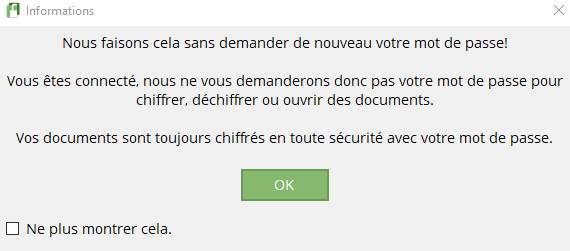
Le mot de passe utilisé pour créer le compte est donc très important. On pourrait donc utiliser un gestionnaire de mot de passe pour pouvoir le retenir.

## 1.2 Réalisation de chiffrement à l’aide d’un mot de passe

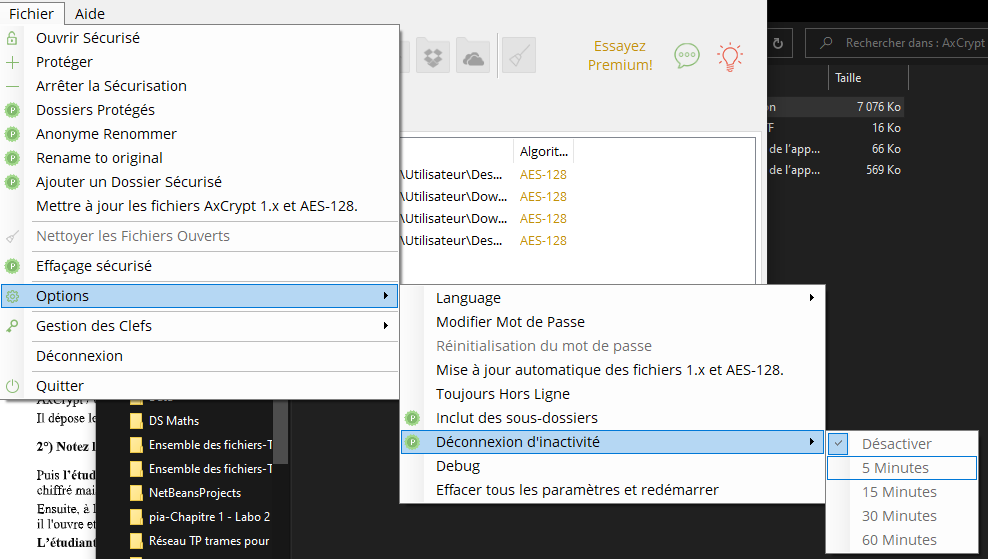
2°) Du côté de **l’étudiant A**, une fois AxCrypt mis en place, pour crypter un fichier, il faut cliquer droit sur le document qui nous intéresse et sélectionner AxCrypt -> **Crypter**.



Il est à noter qu’AxCrypt nous indique qu’il ne demandera le mot de passe qu’une fois par session.



Si l’on veut renforcer la sécurité, il est possible d’indiquer à AxCrypt de déconnecter l’utilisateur dans l’onglet « Fichier -> Options -> Déconnexion d’inactivité » pour que le logiciel redemande le mot de passe après un certain temps d’inactivité sur la session.

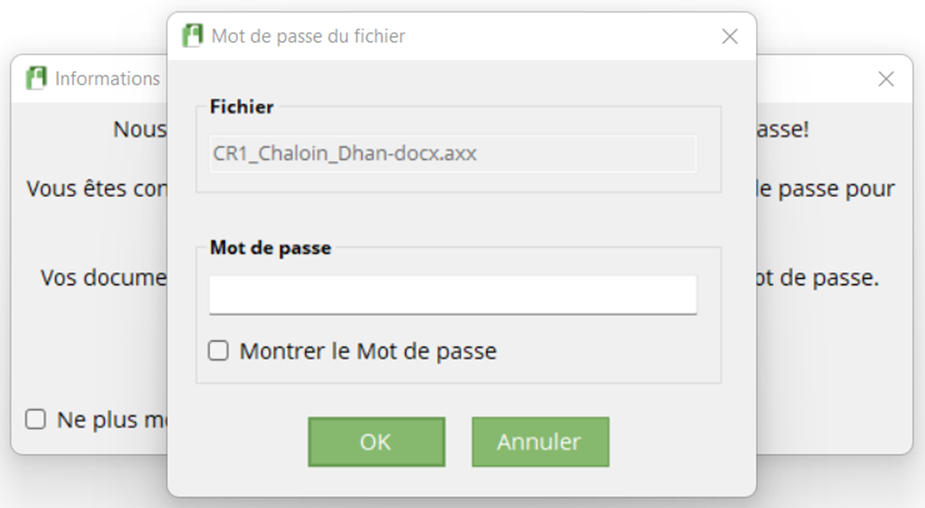


Une fois le fichier crypté, il sera sous une nouvelle extension .axx.



Ce fichier ne pourra donc être lu qu’avec le mot de passe définit, et est donc sécurisé. **L’étudiant A** peut donc le mettre sur un Google Drive pour le partager avec **l’étudiant B**.

3°) L’étudiant B récupère donc le fichier crypté sur le Google Drive. En tentant de l’ouvrir, il reçoit le message suivant :

  
**L’étudiant A** doit donc fournir le mot de passe qu’il a utilisé pour crypter le fichier à **l’étudiant B.** Cependant, on ne peut pas le donner via le même canal que celui utilisé pour le fichier : Cela rendrait le chiffrage du fichier inutile si une personne malveillante intercepte l’échange et qu’elle puisse obtenir le fichier ainsi que le mot de passe pour le déchiffrer.

Il est ainsi nécessaire que **l’étudiant B** reçoive le mot de passe dans un canal de communication différent.

**L’étudiant B** utilise donc le mot de passe fournit par l’**étudiant A** et déchiffre le fichier, ce qui lui permet de l’ouvrir et d’y apporter des modifications. L’**étudiant B** n’aura pas besoin de réencrypter le fichier, le logiciel le fera lui-même en gardant le même mot de passe attribué par l’**étudiant A**.

L’**étudiant B** renvoie donc le fichier modifié et chiffré sur le Google Drive, que l’étudiant A récupère et, avec le même mot de passe, le déchiffre.

Cependant, on remarque un problème évident : Un même mot de passe servant pour celui du compte est utilisé pour chiffrer et déchiffrer le document, ce qui veux dire que l’on doit donner au destinataire le mot de passe nécessaire pour déchiffrer le document… ainsi que pour se connecter au compte de l’envoyeur. Ce système est simple et efficace lorsque l’on envoie un fichier à une personne de confiance, mais dès lors qu’il faut l’envoyer à plusieurs personnes, cela devient vite difficile à gérer et risque des fuites.

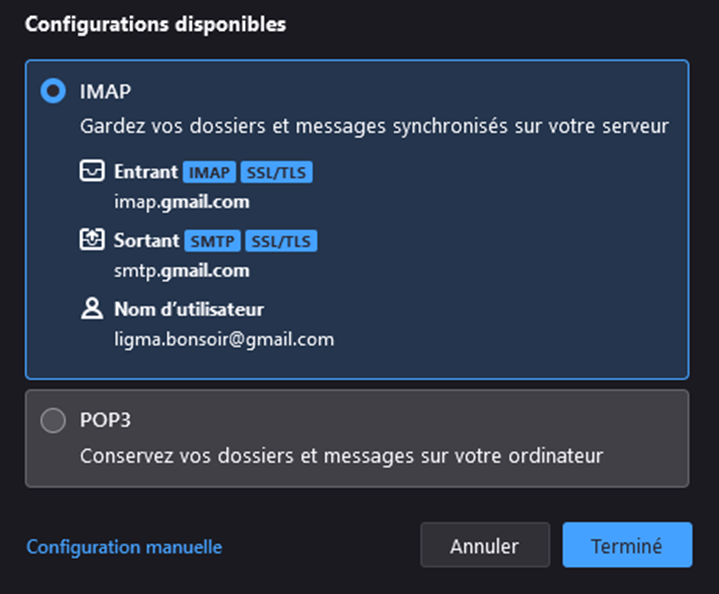
## 

Dans un contexte professionnel, il serait donc intéressant de se pencher plutôt sur le chiffrement asymétrique.

PARTIE 2 Chiffrement asymétrique dans un échange de mail

## 2.1 Installation de Thunderbird et tests

1°) Lors de l’installation de Thunderbird, le logiciel proposera une configuration de la boîte mail :



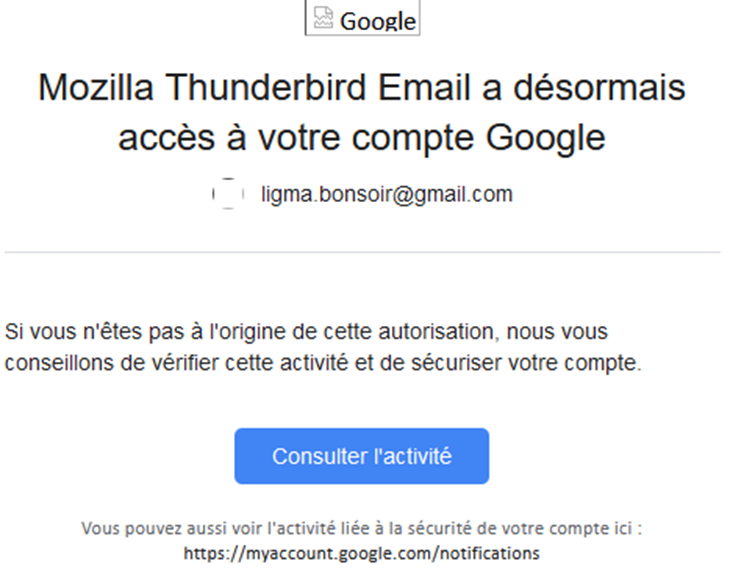
2°) Il est important de savoir la différence entre ces deux protocoles :

-le protocole IMAP relève les courriels en synchronisant les messages sur un serveur, offrant l’avantage de pouvoir consulter un même mail sur différents appareils connectés sur le compte.

-le protocole POP3 relève les courriels, mais une fois qu’ils ont été récupérés du serveur, il les supprime pour les stocker uniquement sur le poste utilisé, ne permettant pas la synchronisation.

Ces deux protocoles sont dits « entrant », permettant la réception des messages dans la boîte mail de l’utilisateur. Le protocole SMTP, commun aux deux options, est dit « sortant », car c’est celui qui s’occupe de transmettre le message entre les différents serveurs jusqu’au destinataire du message.

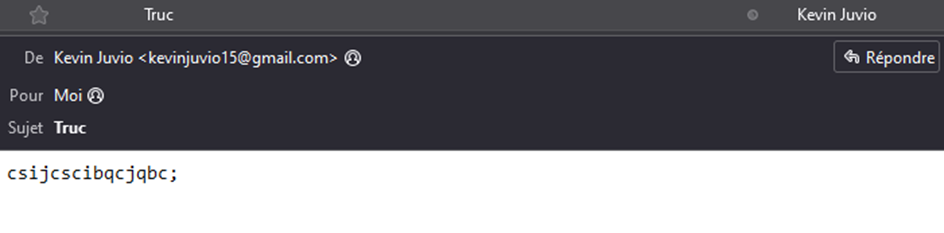
1°) Une fois l’adresse Gmail fournie à Thunderbird, Google envoie immédiatement le mail suivant :



Thunderbird doit pouvoir accéder aux mails envoyés à l’adresse mail dont le compte Google est associé. L’utilisateur sait qu’il est à l’origine de l’autorisation, il peut donc l’ignorer. Il faudra cependant suivre les instructions de ce mail dans le cas où l’utilisateur reçoit ce mail sans en avoir donné l’autorisation, qui pourrait indiquer une attaque sur son adresse mail.

4°) Pour vérifier que le logiciel est correctement paramétré pour l’envoi et la réception de messages, les deux étudiants établissent un test d’envoi et de réception.

Ici, l’étudiant B envoie à l’étudiant A un mail simple.



Les paramètres de base devraient pouvoir permettre correctement l’envoi et la réception.

## 2.2 Gestion initiale des clés

Pour commencer nous avons paramétrer la section chiffrement de bout en bout. Grâce a cela nous avons réussi a obtenir une paire de clé constitué d’une clé publique et d’une clé publique.

Une image contenant texte

Description générée automatiquement

Voici ci-dessus la première étape pour permettre la création de la paire de clé.

Puis pour la suite des différentes étape, nous pouvons lors de la création créer une date de fin pour que les 2 clés créer sois effacé. Nous avons donc choisi de mettre 5 jour au total pour cas la fin du travail elles soient effacé et donc inutilisable.

Une image contenant texte

Description générée automatiquementUne image contenant texte

Description générée automatiquement

Désormais, Les clé sont maintenant accessible dans le gestionnaire de clés OpenPGP.

Voici ci-dessus les différentes informations qui sont disponibles sur les 2 clés de chiffrement.

## 2.3 Utilisation des clés dans l’échange sécurisé de données

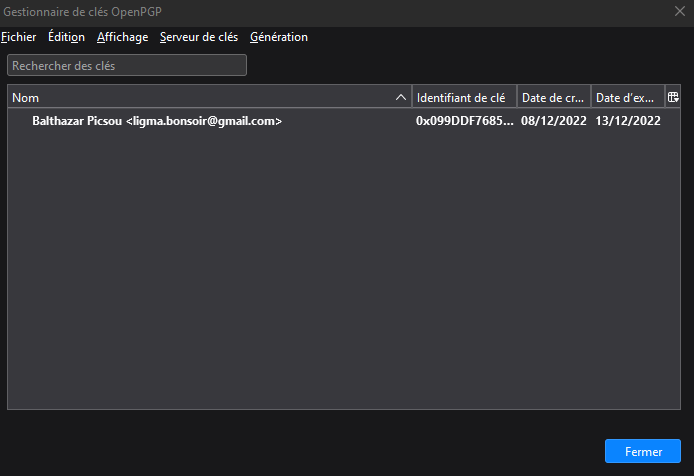
## Question 7

Un jeu de clefs se compose de deux clefs :

- Une clé publique que vous pouvez donner à tout le monde.

- Une clé privée que vous êtes le seul à avoir.

Dans un premier temp nous avons envoyé notre clé publique a notre binôme pour ensuite permettre l’envoie des mails chiffrés.

 Une image contenant texte

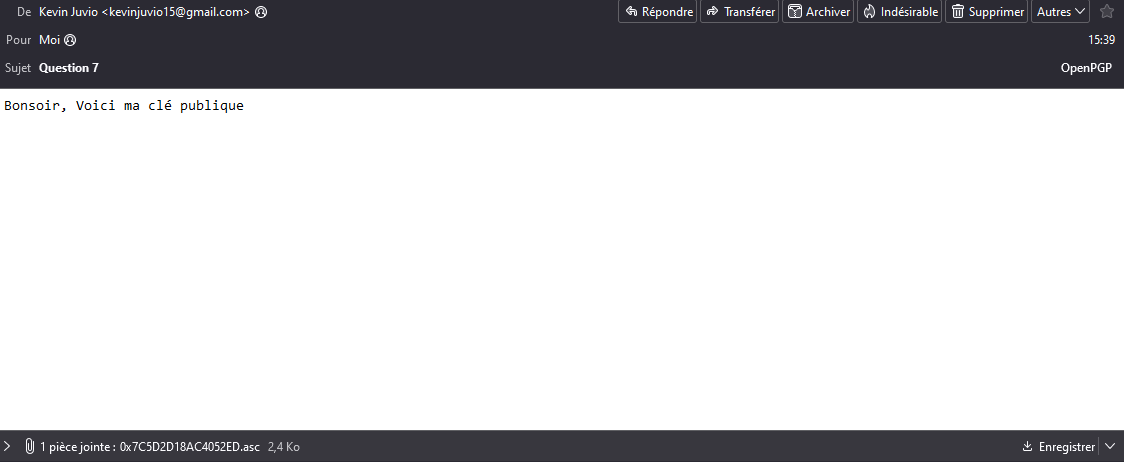
Description générée automatiquement

Pour effectuer cela nous nous somme envoyer un mail avec à l’intérieur notre clé publique en piece-jointe.

## Question 8

La clé publiquepermet de chiffrer un message ou un document, tandis que la clé privée permet de le déchiffrer. Ceci garantit que seul le destinataire choisi peut déchiffrer et lire le contenu. Il est impossible de deviner la clé privée à partir de la clé publique. C'est pourquoi les clés publiques peuvent être partagées sans danger, permettant ainsi aux utilisateurs de bénéficier d'une méthode facile et pratique de chiffrement de contenu et de vérification de signature numérique. Les clés privées restent secrètes, ce qui garantit que seul leur propriétaire peut déchiffrer du contenu et créer des signatures numériques.

## Question 9

Pour pouvoir récupérer la clé publique de son binôme, il suffit de l’envoyer par mail. Il y a aussi d’autre possibilité d’envoie mais vu que nous étions à côté il n’y avait aucun risque pour l’authentification de notre clé publique. 

Voici le Mail contenant un texte et une pièce jointe qui correspond à notre clé publique. Grâce à celle-ci nous pourrons par la suite déchiffrer des messages cryptés.

Question 10 : En fonction des exigences de notre modèle de risque et de nos possibilités, on pourra choisir différentes façons pour vérifier l'authenticité d'une clé publique. Lorsque c'est possible, le plus simple est de se passer en main propre, à l'aide d'une clé USB par exemple, le fichier contenant la clé publique. Mais l’un des inconvénients de la méthode est qu'elle nécessite de se passer un fichier informatique par un moyen sûr. OpenPGP intègre la notion de confiance transitive avec les [toiles de confiance](https://guide.boum.org/tomes/2_en_ligne/1_comprendre/6_chiffrement_asymetrique/4_authentification/3_wot/). Une fois la clé téléchargée, on peut lister les identités qui ont signé sa clé : ces personnes déclarent publiquement avoir vérifié que cette clé appartient bien à la bonne personne. Si l'on connaît une de ces personnes, ou un tiers qui a confiance en une de ces personnes, OpenPGP peut établir des chemins de confiance entre les identités auxquelles on fait confiance et d'autres avec lesquelles on souhaite communiquer

## Question 11

Pour pouvoir nous envoyer le fichier integrite.txt nous devons utilisé la clé publique de notre binôme. Une image contenant texte

Description générée automatiquement

Voici le mail que nous nous sommes envoyés avec comme pièce jointe le fichier intégrité.txt et la clé publique. Grâce a notre clé privée nous avons donc pu déchiffrer le message ainsi que son contenue.

## Question 12 :

## 

Voici un test du décryptage du mail représenté ci-dessus. Il possède toutes les informations concernant les deux clés. Grace a celle-ci le déchiffrement a pu être effectué.

## Question 13 :

Une image contenant texte

Description générée automatiquement

Voici le résultat finale grâce au déchiffrage vu précédemment sur les screens pris, le fichier intégriter.txt a bien pu être ouvert avec le texte a l’intérieur qui a été écris par le second binôme.

## Conclusion :

Nous pouvons en conclure que grâce à ce travail nous savons maintenant crypté mais aussi décrypter des messages qu’ils soient professionnels ou non. Ceci peut être très important pour notre future profession car il va permettre de sécuriser et d’authentifié les documents importants que nous devons fournir. Cela nous a aussi permis d’acquérir de nouvelle connaissance et a nous amélioré dans notre organisation lors d’un travail de groupe.