Table des matières

[**Introduction 3**](#_heading=h.7me5y16q6mru)

[**I. Le chiffrement symétrique avec AxCrypt 3**](#_heading=h.tc9lt9o76rj)

[1.1 Mise en place d’un logiciel de chiffrement de fichiers 3](#_heading=h.6q61g5lqv4so)

[1.2 Réalisation de chiffrement à l'aide d'un mot de passe 5](#_heading=h.qfcqon6me109)

[**II. Chiffrement asymétrique dans un échange de mail 8**](#_heading=h.94a6js9ld0y3)

[2.1 Installation de Thunderbird et tests 8](#_heading=h.und7xpmtq6mz)

[2.2 Gestion initiale des clés 10](#_heading=h.s2oot0gigm3c)

[2.3 Utilisation des clés dans l’échange sécurisé de données 12](#_heading=h.nrd6r5gwheu6)

[2.3.1 - Partager la clé publique 12](#_heading=h.2xbwsh79gth8)

[2.3.2 - Importer la clé publique d’un correspondant 12](#_heading=h.rb8bmm16f0jy)

[2.3.4 -Déchiffrer le document chiffré reçu 14](#_heading=h.jpqatgs0zl7x)

[**Conclusion 16**](#_heading=h.yv4p6yljtgw7)

# 

# 

# Introduction

Ce devoir a été réalisé pour explorer les concepts fondamentaux de la sécurité informatique, en particulier les techniques de chiffrement symétrique et asymétrique. L'objectif était de mettre en pratique ces concepts à travers l'utilisation d'outils concrets comme AxCrypt pour le chiffrement de fichiers et Thunderbird avec OpenPGP pour la sécurisation des échanges par e-mail. Cette approche pratique permet de mieux comprendre les enjeux de la protection des données dans un contexte de communication numérique.

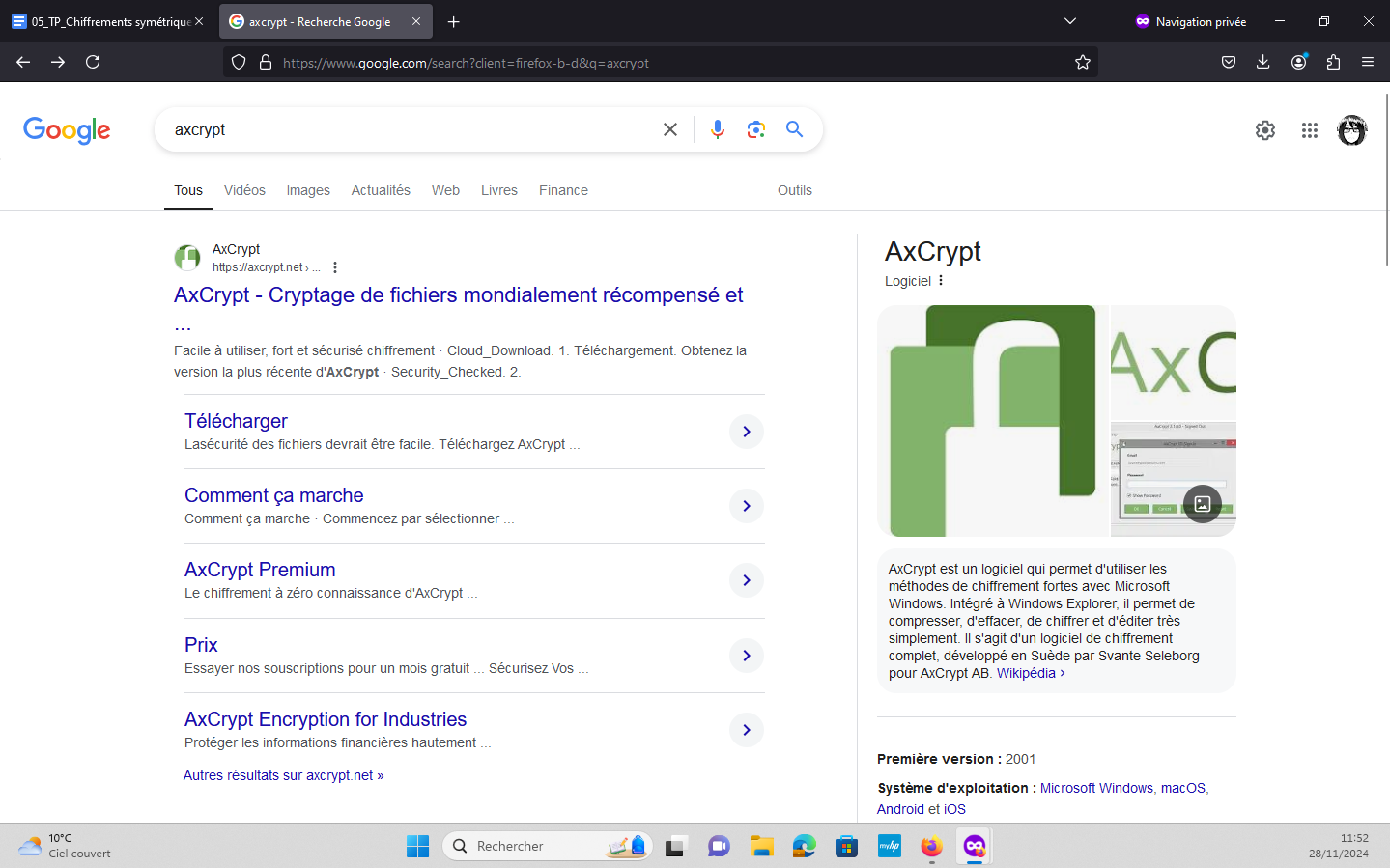
# Le chiffrement symétrique avec AxCrypt

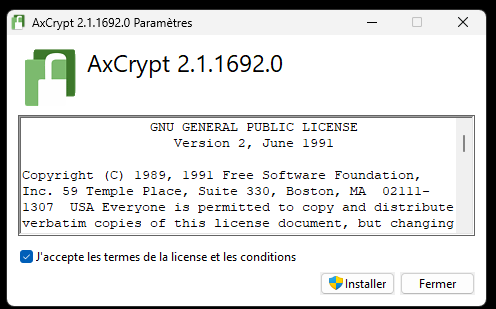
## 1.1 Mise en place d’un logiciel de chiffrement de fichiers

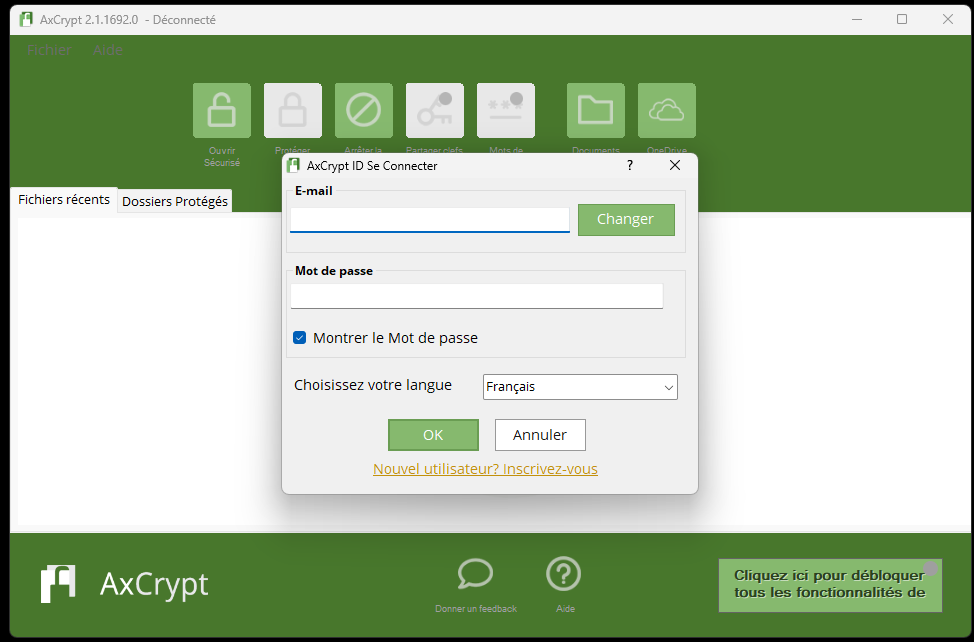
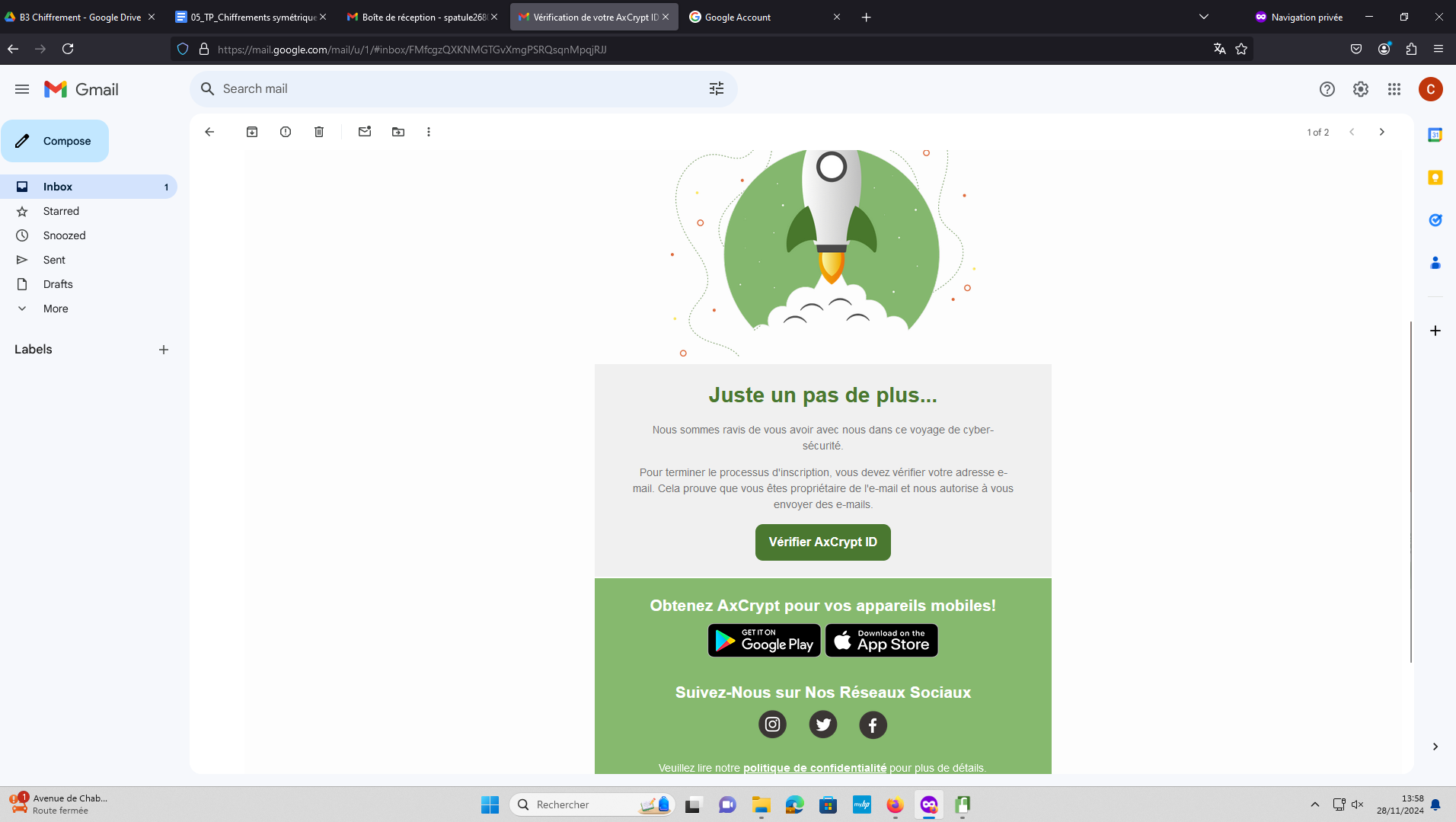
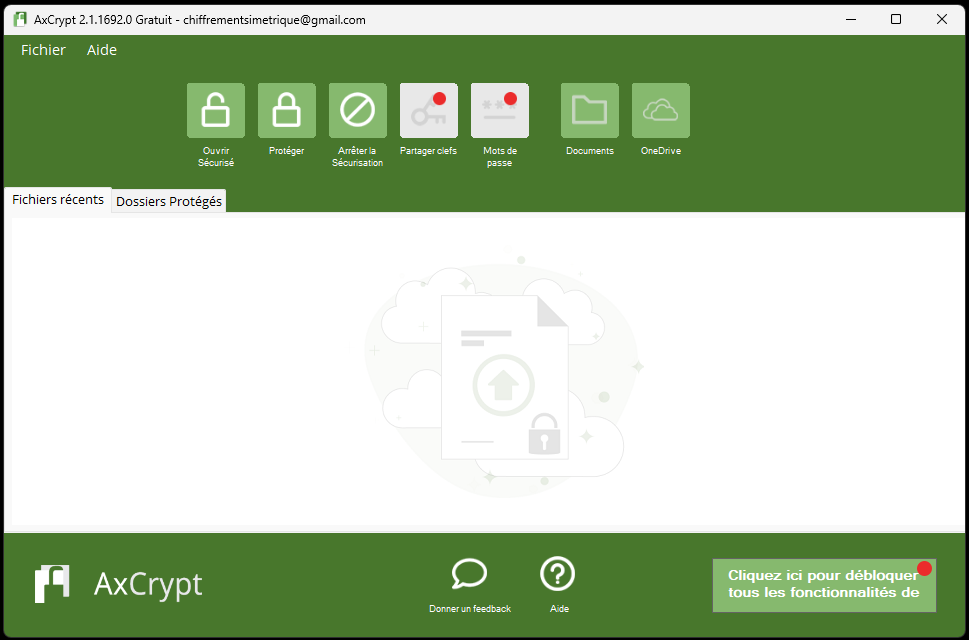
AxCrypt est un logiciel de chiffrement de fichiers ou dossiers sous Windows. Il utilise l'algorithme AES-128 (version gratuite).

L'utilisation de ce type de logiciel est simple. Il permet le chiffrage et déchiffrage de fichier à l'aide d'un mot de passe.

Les deux étudiants installent AxCrypt-2.1.1573.0.exe sur leur poste personnel (fichier présent dans le dossier fourni). Bien évidemment il ne faut installer que ce qui est strictement nécessaire !

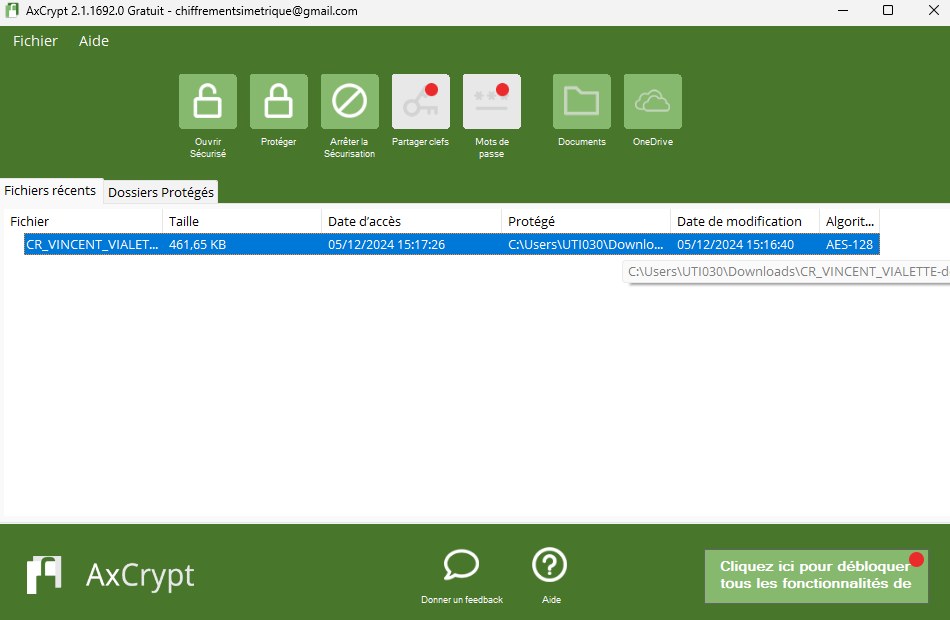
Pour l’installation d’AxCrypt, il n’y a rien de plus simple. Tout d’abord, il faut aller sur le site officiel.  


Une fois dessus, allez sur la partie “Télécharger” et prenez la version Windows.  
  
Une fois le téléchargement terminé, lancez l’installeur puis acceptez les termes de la licence et les conditions générales d'utilisation.  


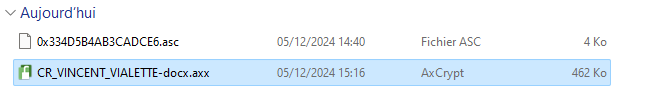
Une fois sur AxCrypt, vous allez avoir besoin d’un compte AxCrypt pour utiliser ce logiciel.  
  
  
Ainsi, rendez-vous sur le site et créez un compte. Après la création du compte, vous recevrez un mail de confirmation ce qui peut prendre plus ou moins de temps, il est important de bien regarder les spams.  
Vous voilà prêt à chiffrer vos fichiers pour les envoyer de manière sécurisée !  


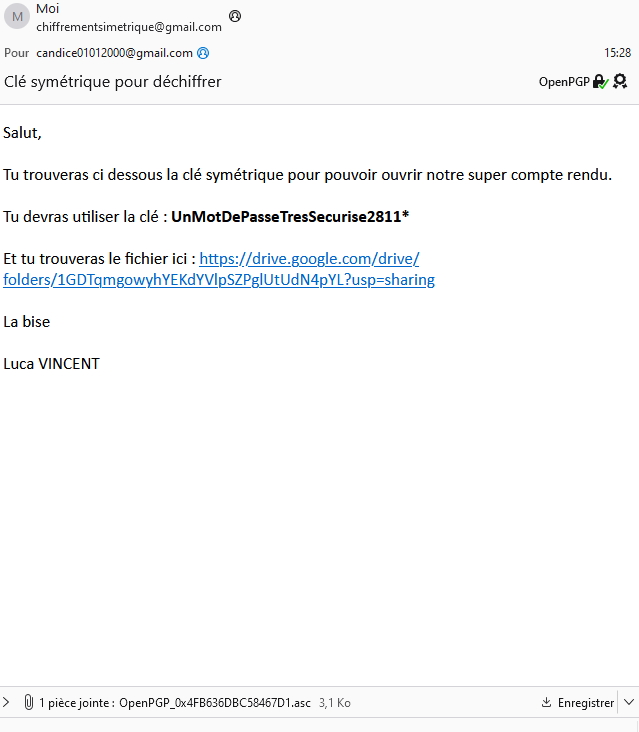
## 1.2 Réalisation de chiffrement à l'aide d'un mot de passe

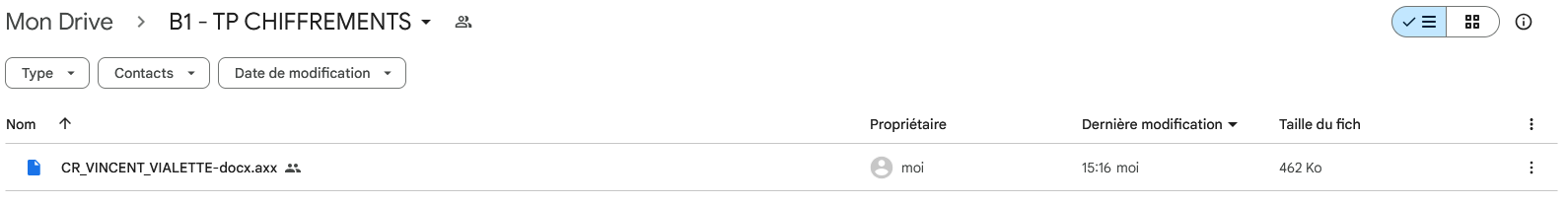
AxCrypt est très instinctif pour chiffrer des fichiers. Il suffit de cliquer sur sur protéger et sélectionner le fichier que l’on veut chiffrer. Il sera donc affiché sur le logiciel.



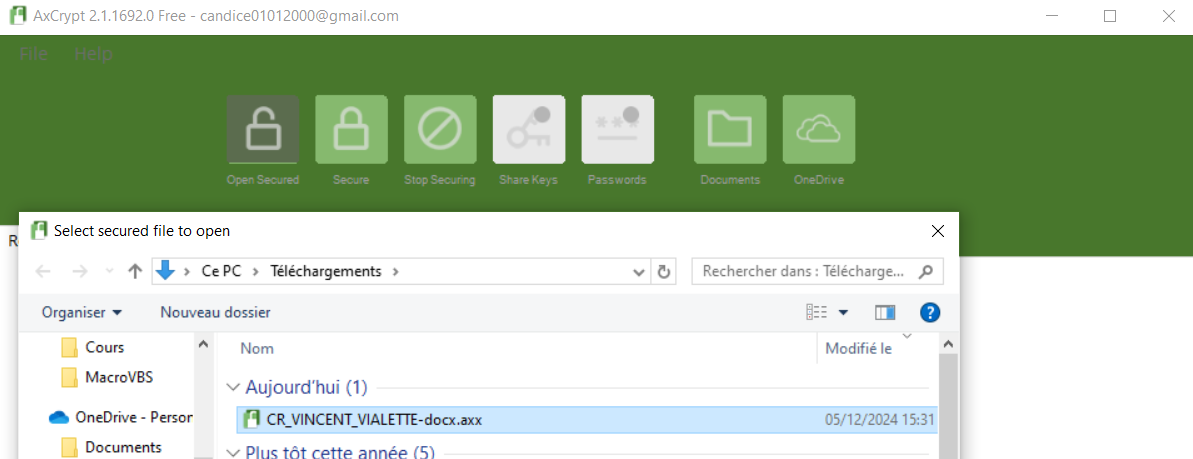
Lorsqu’on regarde l’emplacement du fichier, on peut s'apercevoir que l’icône ainsi que l’extension ont totalement changé. On passe d’un fichier .docx en un fichier en .axx.

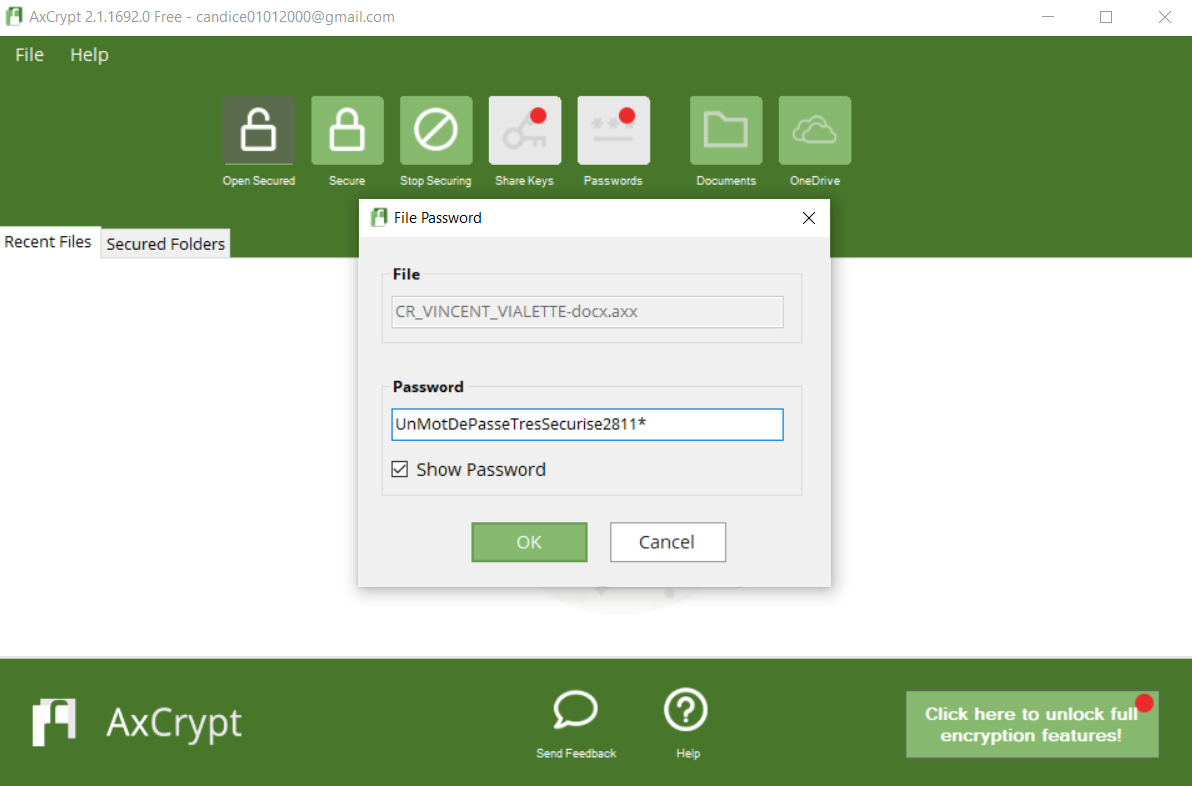


Pour envoyer la clé de chiffrement, nous avons utilisé Thunderbird en chiffrant le mail. La clé de chiffrement et de déchiffrement correspondent au mot de passe du compte. J’ai ainsi stocké le fichier contenant le pseudo compte rendu sur un drive et candice et dorénavant en possession de la clé de déchiffrement.   


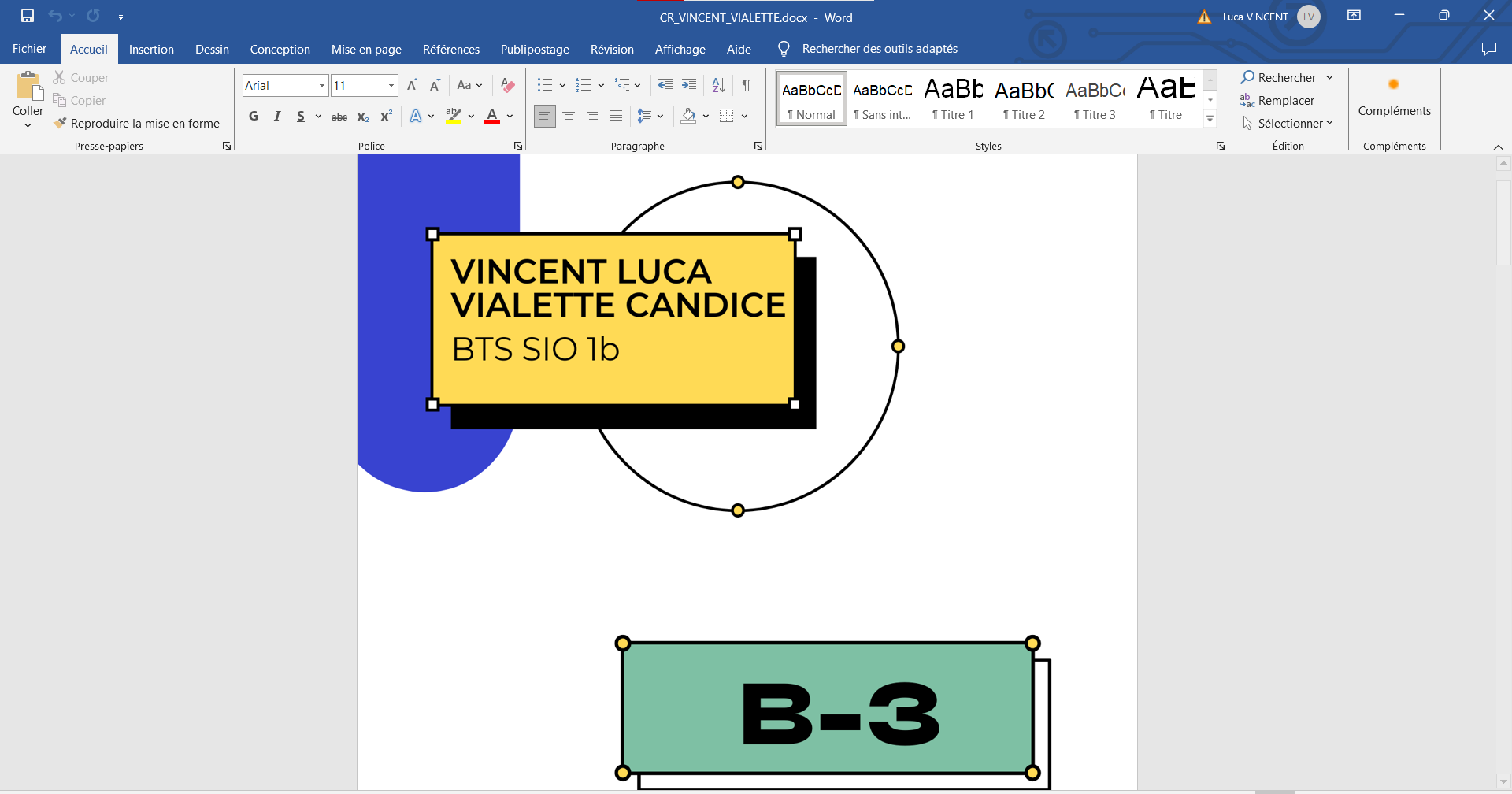


Pour pouvoir lire le fichier, la personne qui télécharge le fichier se doit d’avoir AxCrypt d’installé et sous la possession d’un compte. Ainsi il suffira d’ouvrir le compte rendu sur AxCrypt pour pouvoir le déchiffrer.





Une fois la clé de chiffrement entrée, le fichier n’est plus sécurisé et pourra être ouvert en utilisant Word.



# Chiffrement asymétrique dans un échange de mail

## 2.1 Installation de Thunderbird et tests

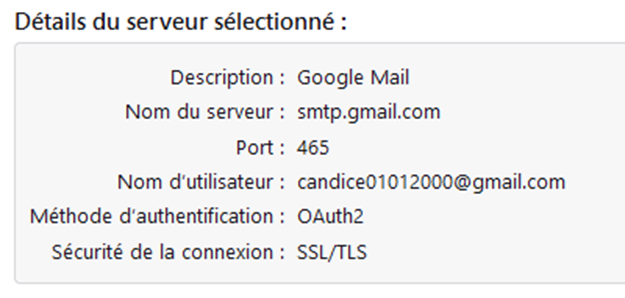
Nous avons utilisé **Thunderbird** comme client de messagerie pour ce TP, en le configurant avec un compte Gmail spécialement créé.

#### **Étapes de l'installation :**

1. **Téléchargement et installation de Thunderbird** :
   * Rendez-vous sur le site officiel de Thunderbird pour télécharger la dernière version.
   * Lancez l'installation en suivant les étapes proposées et acceptez les conditions générales d'utilisation.
2. **Paramétrage du compte Gmail** :
   * Configurez un compte Gmail avec les identifiants fournis.
   * Attention : Gmail peut envoyer une alerte concernant la connexion. Veillez à interpréter ce message correctement.

#### **Rôles des protocoles IMAP, POP3, et SMTP :**

* **SMTP** : Envoi des e-mails à leurs destinataires :



* **POP3** : Télécharge les e-mails sur l’appareil local et les supprime du serveur :



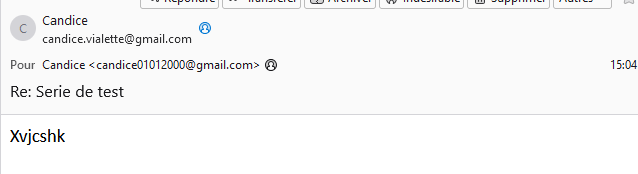
* **IMAP** : Permet de lire les e-mails sur plusieurs appareils sans les supprimer du serveur :



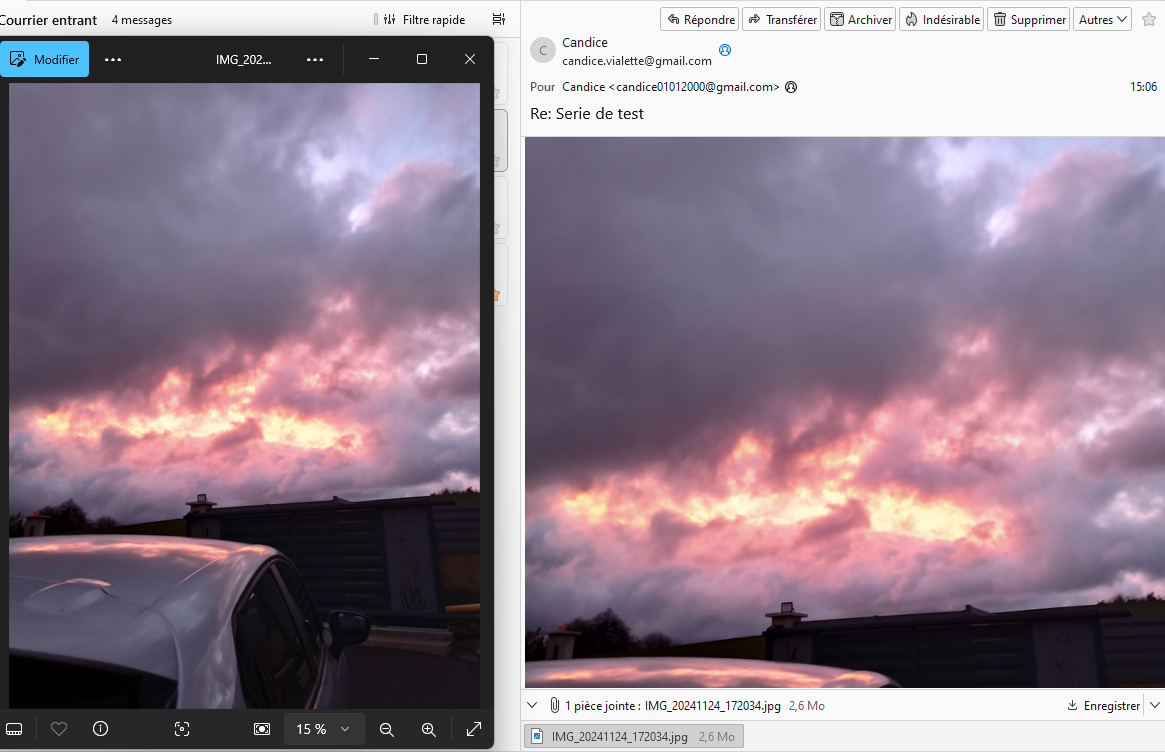
#### **Tests d’envoi et de réception :**

Nous avons effectué des tests d’envoi et de réception avec des textes et des images. Les messages circulaient sans problème, confirmant que la configuration était correcte :

Mail de texte entrant :



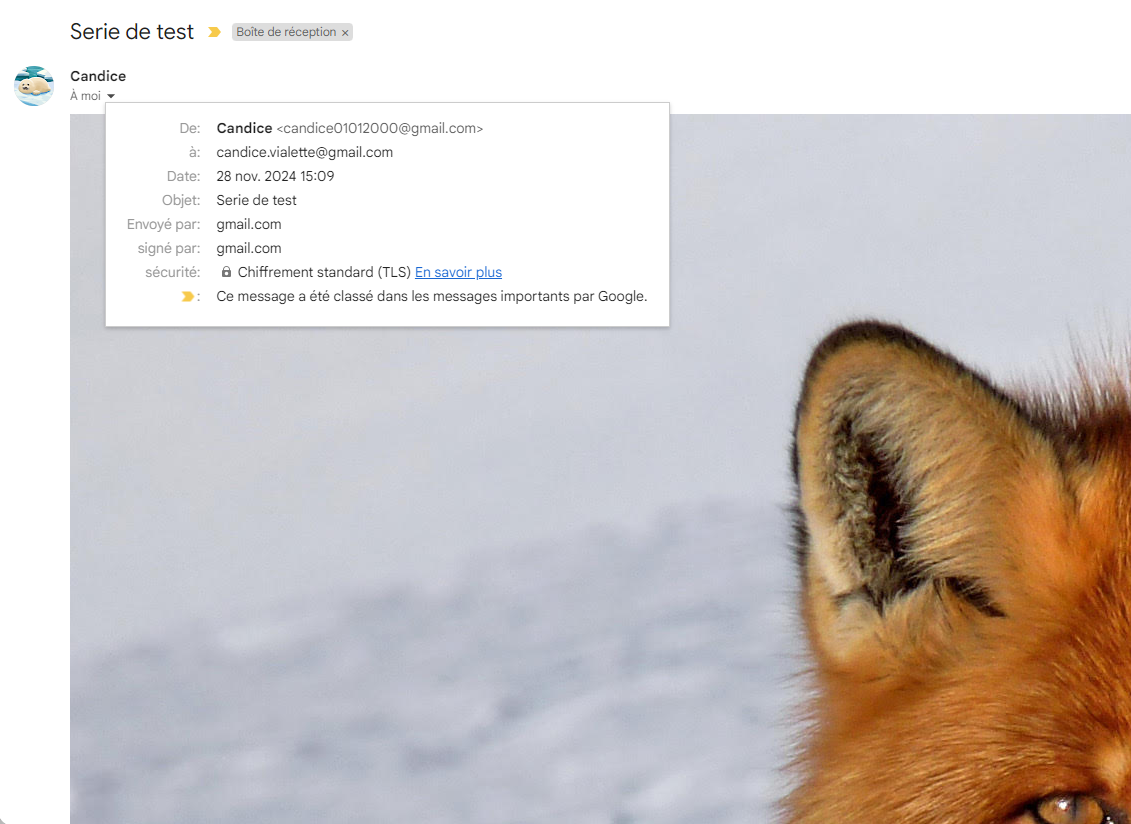
Mail d’une image entrante :



Mail d’un texte sortant (reçu par le destinataire) :



Mail d’une image sortant (reçu par le destinataire) :



Ouverture de l’image du mail du dessus :

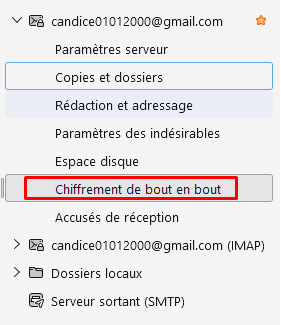


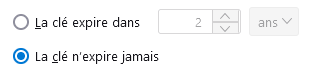
## 2.2 Gestion initiale des clés

Depuis la version 78, Thunderbird intègre OpenPGP pour le chiffrement asymétrique.

#### **Étapes pour générer et configurer les clés :**

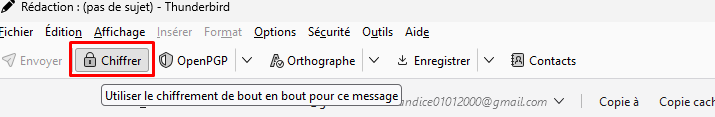
1. **Accéder aux paramètres OpenPGP** :
   * Ouvrez les paramètres du compte dans Thunderbird.
   * Activez le chiffrement de bout en bout et sélectionnez « Ajouter des clés » :



1. **Génération des clés** :
   * Sélectionnez une longueur de clé de **4096 bits** pour une sécurité renforcée : 
   * Configurez une durée de validité (illimitée dans notre cas) : 
   * Exportez la clé privée pour une sauvegarde :



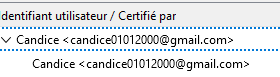
1. **Configuration des envois** :
   * Activez l’option pour signer et chiffrer automatiquement tous les e-mails :

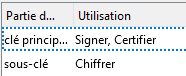


Les clés générées contiennent des informations : 

Il y a le type de clé (clé public et sécrète), son identifiant, son empreinte, sa date de création et sa date d’expiration

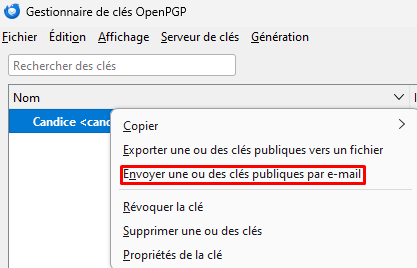
Je la définit comme une clé personnelle

Elle s'identifie et est certifié par moi-même



2.3 Utilisation des clés dans l’échange sécurisé de données

### 2.3.1 - Partager la clé publique

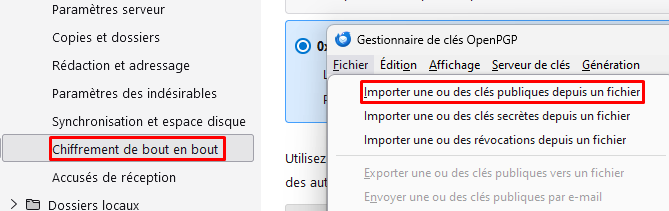
Envoyez la clé publique par e-mail à votre correspondant en pièce jointe. Cela permet de chiffrer les communications et de vérifier les signatures : 



La clé publique permet que le premier échange soit crypté avec une clé connue. Il permet aussi de vérifier que la signature de la personne est authentique, ce qui permet de prouver son identité.

### 2.3.2 - Importer la clé publique d’un correspondant

1. Recevez la clé publique par e-mail ou via un autre moyen sécurisé :

Il doit nous l’envoyer via un canal sécurisé. On va dans les paramètres de compte, dans le chiffrement de bout en bout puis dans gestionnaire de clés OpenPGP. Ensuite on va dans un fichier et on importe une ou des clés publiques depuis un fichier

1. Importez-la dans Thunderbird à l’aide du gestionnaire de clés OpenPGP
2. Vérifiez son authenticité en comparant l’empreinte numérique ou en utilisant une autorité de certification.

Pour vérifier si la clé publique appartient bien à mon correspondant, il faut regarder si le certificat numérique est signé par une autorité de certification de confiance et encore valide. On peut aussi regarder son empreinte (hash) de sa clé publique et les comparer pour vérifier sa correspondance. Partager la clé public sur un canal sécurisé sise la partager hors ligne n’est pas possible.

2.3.3 - Chiffrer un document à l’aide de la clé publique du destinataire

|  | Il est impossible de chiffrer un message sans avoir la clé publique du destinataire. |
| --- | --- |
|  | Avec sa clé, je peux lui envoyer des messages chiffrés. |

### 2.3.4 -Déchiffrer le document chiffré reçu

|  | Le mail est illisible car Gmail ne peut pas déchiffrer des messages et des pièces jointes chiffrées avec OpenPGP car il ne stocke pas ni ne gère les clés privées de ses utilisateurs. |
| --- | --- |

Pour le lire, il faut :

|  | Maintenant sur Thunderbird, on peut voir le contenu du message car il y a la clé public dedans |
| --- | --- |
|  | Sur Gmail, le mail que j’ai écrit ne peut pas être chiffré car il ne peut pas contenir ma clé privée ni aucune clé de chiffrement. |

# Conclusion

Ce travail nous a permis de développer une compréhension approfondie des mécanismes de chiffrement symétrique et asymétrique, ainsi que de leur application dans la sécurisation des données. Grâce à l'utilisation d'AxCrypt pour le chiffrement de fichiers, nous avons appris à protéger des informations sensibles à l'aide d'un mot de passe, ce qui souligne l'importance de la sécurité des fichiers dans un environnement numérique.   
  
De plus, l'intégration de Thunderbird avec OpenPGP pour les échanges d'e-mails a enrichi notre connaissance des protocoles de sécurité. Nous avons découvert comment générer et gérer des clés publiques et privées, ce qui est essentiel pour assurer la confidentialité et l'intégrité des communications. Ce processus nous a également sensibilisés aux enjeux liés à la vérification d'identité et à la protection contre l'usurpation.   
  
En conclusion, ce travail pratique a non seulement renforcé nos compétences techniques en matière de sécurité informatique, mais il a également mis en lumière l'importance cruciale de ces pratiques dans la protection des données personnelles et professionnelles dans notre monde numérique.