# Cryptographie asymétrique (à clé publique)



## Activité :

S’informer sur les caractéristiques de l’algorithme de chiffrement RSA. Présenter la mise en œuvre des algorithmes de chiffrement symétrique et asymétrique dans le protocole SSH.

Liens :

* CNIL :
	+ Comprendre les grands principes de la cryptologie et du chiffrement : <https://www.cnil.fr/fr/cybersecurite/comprendre-les-grands-principes-de-la-cryptologie-et-du-chiffrement>
* Clarification de l’ANSSI sur l’utilisation des clé cryptographique RSA 2048 bits :
	+ <https://cyber.gouv.fr/sites/default/files/document/Note-clarification-utilisation-RSA-2048-bits-PSCo-qualifies.pdf>
* Etablissement d'une connexion SSH :
	+ <https://www.hostinger.com/fr/tutoriels/ssh-linux>
* Sécuriser un accès SSH :
	+ <https://www.it-connect.fr/chapitres/bonnes-pratiques-de-configuration-ssh/>

### Questions :

* Quels sont noms des inventeurs de l’algorithme de chiffrement RSA et à quelle date ont-ils publiés le principe de cet algorithme ?
* Quels sont les deux usages de ce chiffrement asymétrique ?
* Quelles est la longueur des clés que recommande l’ANSSI en France pour la période actuelle et pour les prestataires de services de confiance ?

Le protocole SSH permet de se connecter en mode texte (shell) avec un serveur :

* Etape 1 : en créant un canal de communication sécurisé entre le client et le serveur ,
* Etape 2 : en permettant une authentification par login /mot de passe ou par clé SSH.

SSH peut aussi permettre la création d’un tunnel sécurisé pour d’autres services : SSH File Transfer Protocol (soit SSH FTP) transfert de fichiers à travers SSH ; Secure copy (scp) : transfert de fichiers à travers SSH.

### Questions : Réalisez un schéma décrivant les étapes de la création d'un canal sécurisé avec SSH, depuis la sécurisation des échanges jusqu'à l'authentification sous forme de diagramme de séquence, en utilisant la solution en ligne **PlanUML**.

* Site de PlantUML : <https://plantuml.com/fr/>
* Le guide de PlantUML : <http://plantuml.com/fr/guide>
* Le site pour la création du diagramme en ligne de PlantUML : <http://www.plantuml.com/plantuml/uml/>