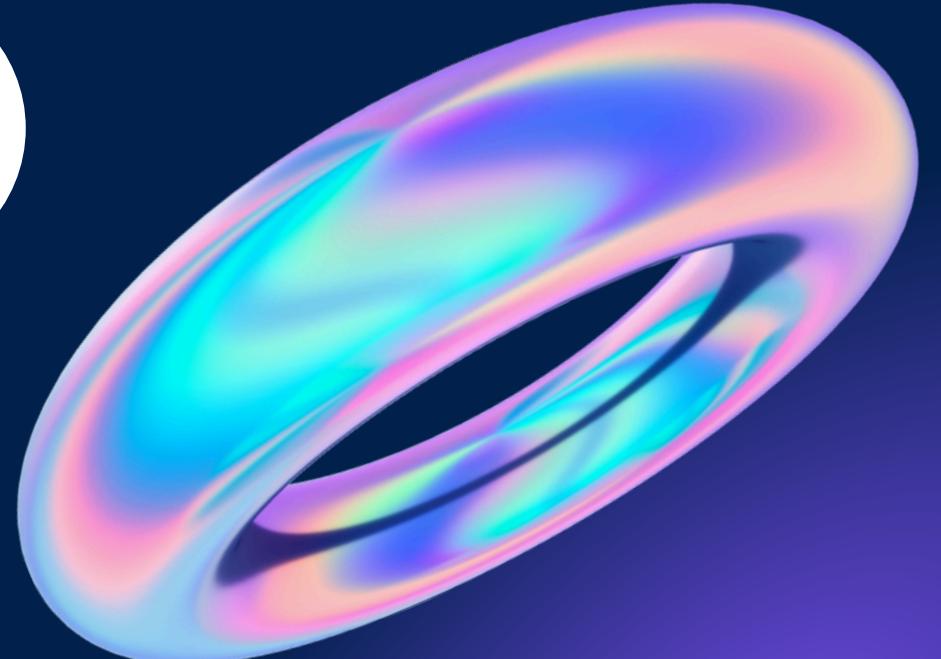


Mercredi 9 octobre 2024



# Bienvenue!

**SÉANCE 05:** Brute force, élévation  
des priviléges

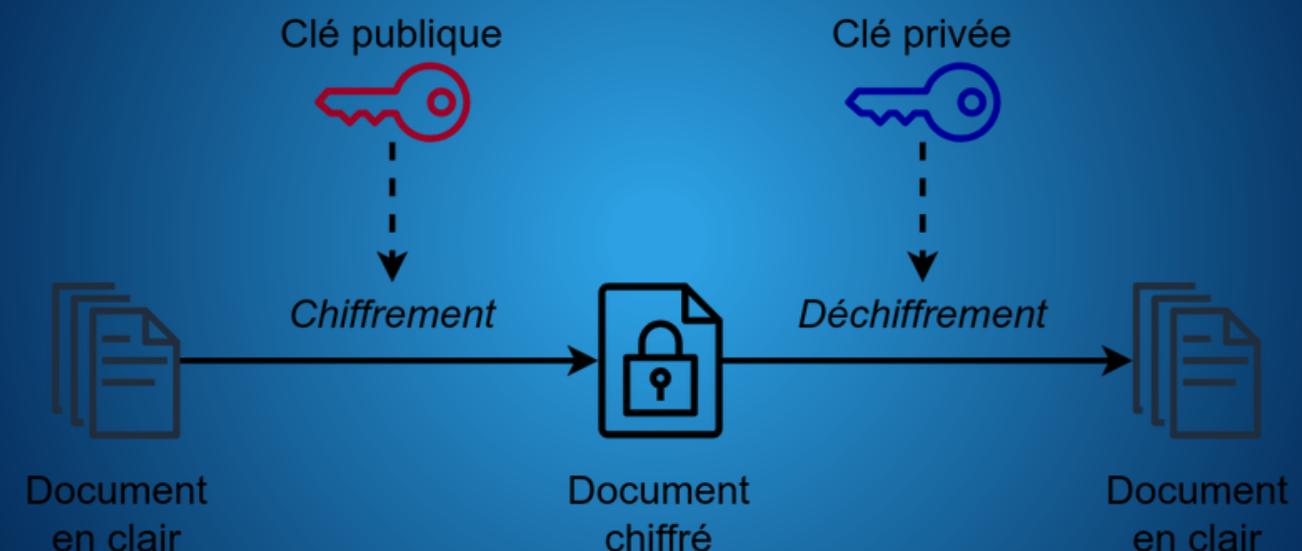


# Connexion SSH

Par défaut, utilisation d'un **mot de passe**.

→ L'authentification par échange de **clés SSH** offre plus de sécurité.

## Cryptographie asymétrique



*Exemples d'algorithmes:*

- DSA
- RSA
- EdDSA

# Connexion SSH

Exemple de **RSA** (Ron Rivest, Adi Shamir et Leonard Adleman, 1977)

repose sur la **difficulté de factoriser un grand nombre en deux nombres premiers** (problème dans NP)

$$n = pq$$

*la sécurité des clés RSA dépend largement de leur longueur*

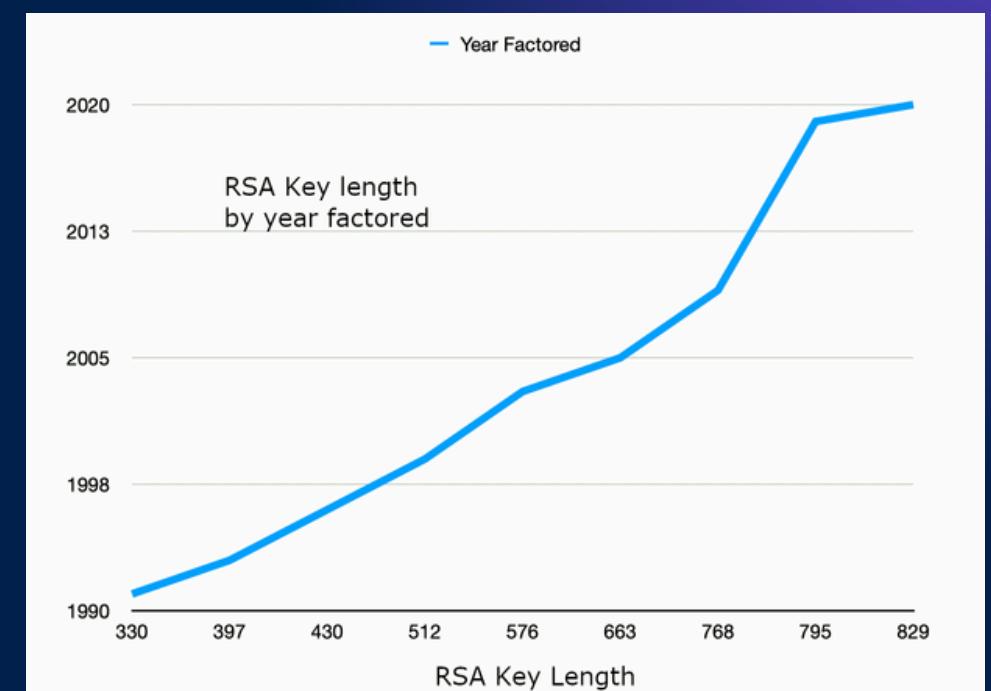
## Échange des clés RSA

Sur votre machine:

- **~/.ssh/id\_rsa** : votre clé privée
- **~/.ssh/id\_rsa.pub** : votre clé publique

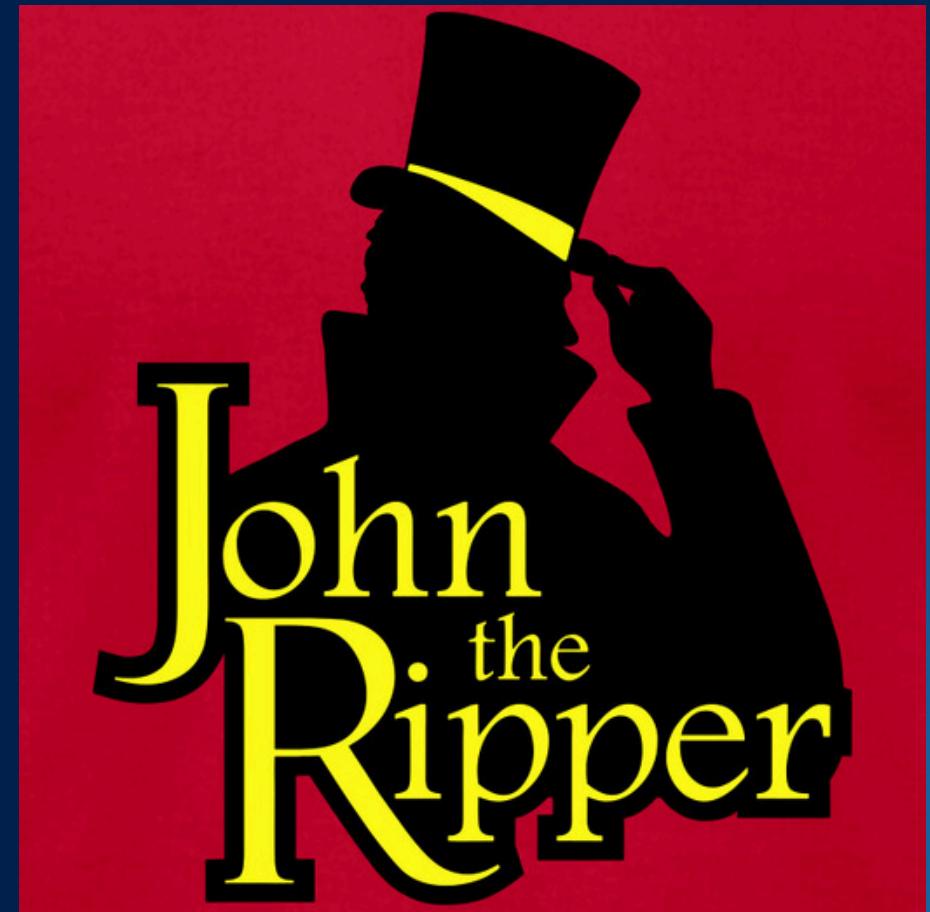
Sur le serveur:

- **~/.ssh/authorized\_keys** : liste des clés publiques autorisées pour se connecter à l'utilisateur (c'est ici que vous devez placer votre clé publique)



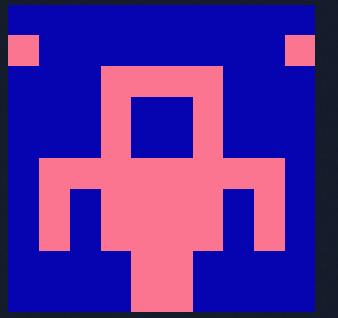
# John The Ripper

→ Casser des mots de passe et  
des hashes par force brute



*Autodétection des fonctions de hachage utilisées (MD5, SHA, Blowfish, etc.).*

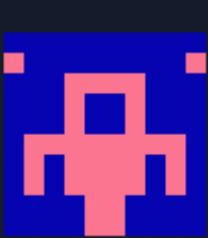
# La room du jour



## Brute It

Learn how to brute, hash cracking and escalate privileges in this box!

||| Easy ⏰ 0 min



## Brute It

Learn how to brute, hash cracking and escalate privileges in this box!

Easy 0 min

# Outils/commandes utiles

nmap

gobuster

> chmod 600 *fichier*

ssh2john

johntheripper

wget

> sudo -l

hydra

gtfobins



<https://github.com/CyberMines-Nancy/SEANCES>

# Merci et à la semaine prochaine !



La séance sur notre Github:  
<https://github.com/CyberMines-Nancy/SEANCES>



@cyber.mines