Tables arc-en-ciel

FAUQUETTE Mael, MAHIER Awen, RABOT Valentin, TRANSON Alexandre

L3 Informatique Groupe 3A

4 avril 2024

UNIVERSITÉ
CAEN
NORMANDIE

Sommaire

Introduction

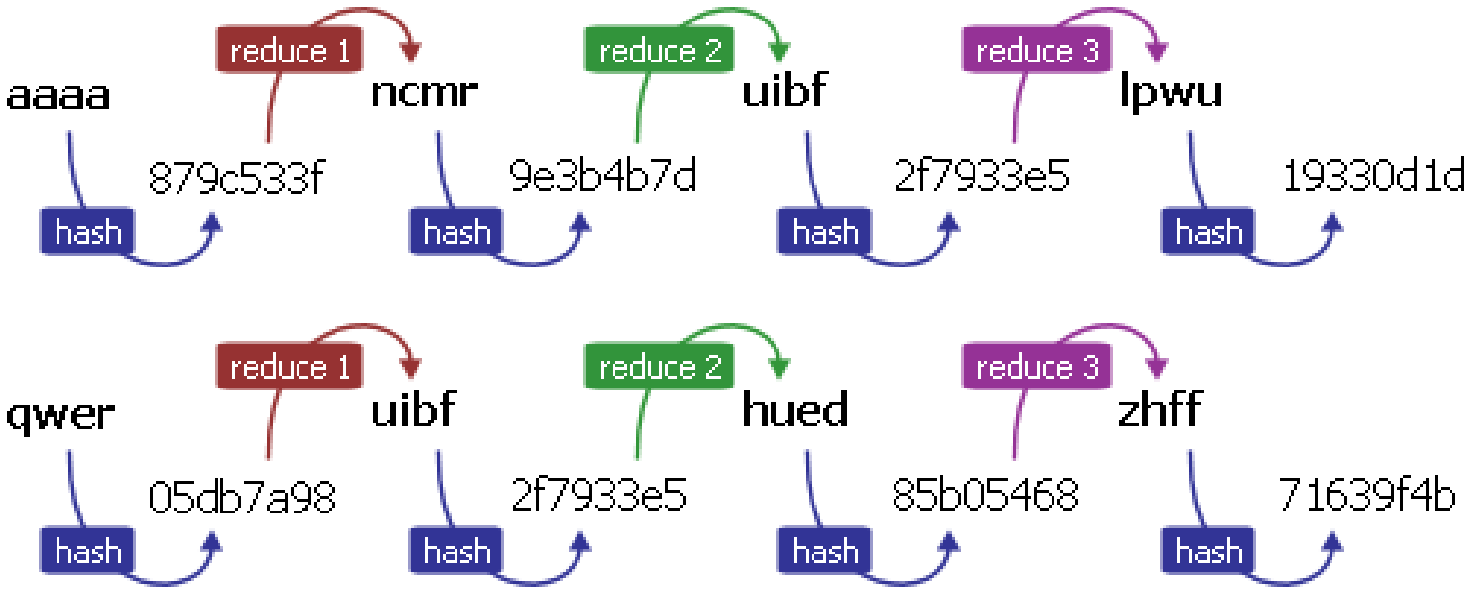
Description du projet

Tables arc-en-ciel

⇒ Structure de données qui réduit les temps de calcul pour retrouver un mot de passe au prix d'un coût en espace.
⇒ Stockent des hashs afin de vérifier facilement si une empreinte existe et son mot de passe correspondant.

Introduction

Tables arc-en-ciel



Rainbow Table

aaaa	19330d1d
qwer	71639f4b

Figure – Génération d'une rainbow table

Problématique

Description de la problématique

Comment créer une table arc-en-ciel fonctionnelle et optimisée ?

Principaux objectifs :

- Générer une base synthétique de mots de passe hachés.
- Implémenter une table arc-en-ciel paramétrable.
- Implémenter des optimisations de la table arc-en-ciel.
- Étude comparative des performances en fonction des paramètres.

Décomposition des tâches

Répartition du travail

- Génération des mots de passe et stockage de leurs hash : Awen
- Fonction de réduction et comparaison des hash : Mael
- Rapport, diaporama et récupération des données : Valentin
- Interface graphique et hachage des mots de passe : Alexandre

Fonctionnalités

Génération des mots de passe

⇒ Parcours d'un hash.
⇒ Calcul d'une graine qui sera utilisée avec la classe Random.
⇒ Une longueur pour le mot de passe entre 8 et 32 caractères.

Fonctionnalités

Dé-hachage d'un mot de passe

Impossible avec un algorithme de hachage sécurisé comme SHA-256. Ce processus est unidirectionnel, il est conçu pour être irréversible.

Fonctionnalités

Stockage des mots de passe

⇒ Dans un fichier texte.
⇒ Première ligne la profondeur et la liste des couleurs.
⇒ Chaque ligne représente un mot de passe d'origine et un hash.

Fonctionnalités

Stockage des mots de passe

```
5 [Purple]
oYI671zd5fTRc 9190b9202f0aaf9ae55292f0eb980848d6d9dc4709ad42a44194cc3d1c8171d3
gR5Ok1M7ti fc923e8132dbfd9d1006ce6cee23d159e0794abcbd54ed19de65440b15b61694
wQcRPKVLhn f9c4ef091c17b37d35b8f410984b7c1e752b4953dccbde53c21a0277feec06fd
JOBq 69eb8919619196e50640fb80d1989eae99eca5d4584c835f1dc92bd50ddc6be8
cvUPQjJXMct3k 31da95a13afc6b52a15f0a02177fa662f14b7769ce4601cceaaba67452977907
```

Figure – Données dans le fichier texte

- Profondeur : nombre d'itérations du processus de compression.
- Couleur(s) : fonction de réduction.

Fonctionnalités

Récupération des données

⇒ BufferedReader pour lire le fichier texte ligne par ligne.
⇒ Première ligne extraite pour obtenir la profondeur et les couleurs.
⇒ Les lignes suivantes sont parcourues.

Fonctionnalités

Comparaison des mots de passe

⇒ Fonctions de réduction pour obtenir le mot de passe.
⇒ Si aucune correspondance :

- Génération de nouveaux hash à partir du hash fourni
- Trouver une correspondance ou atteindre la profondeur maximale

Fonctionnalités

Fonction de réduction

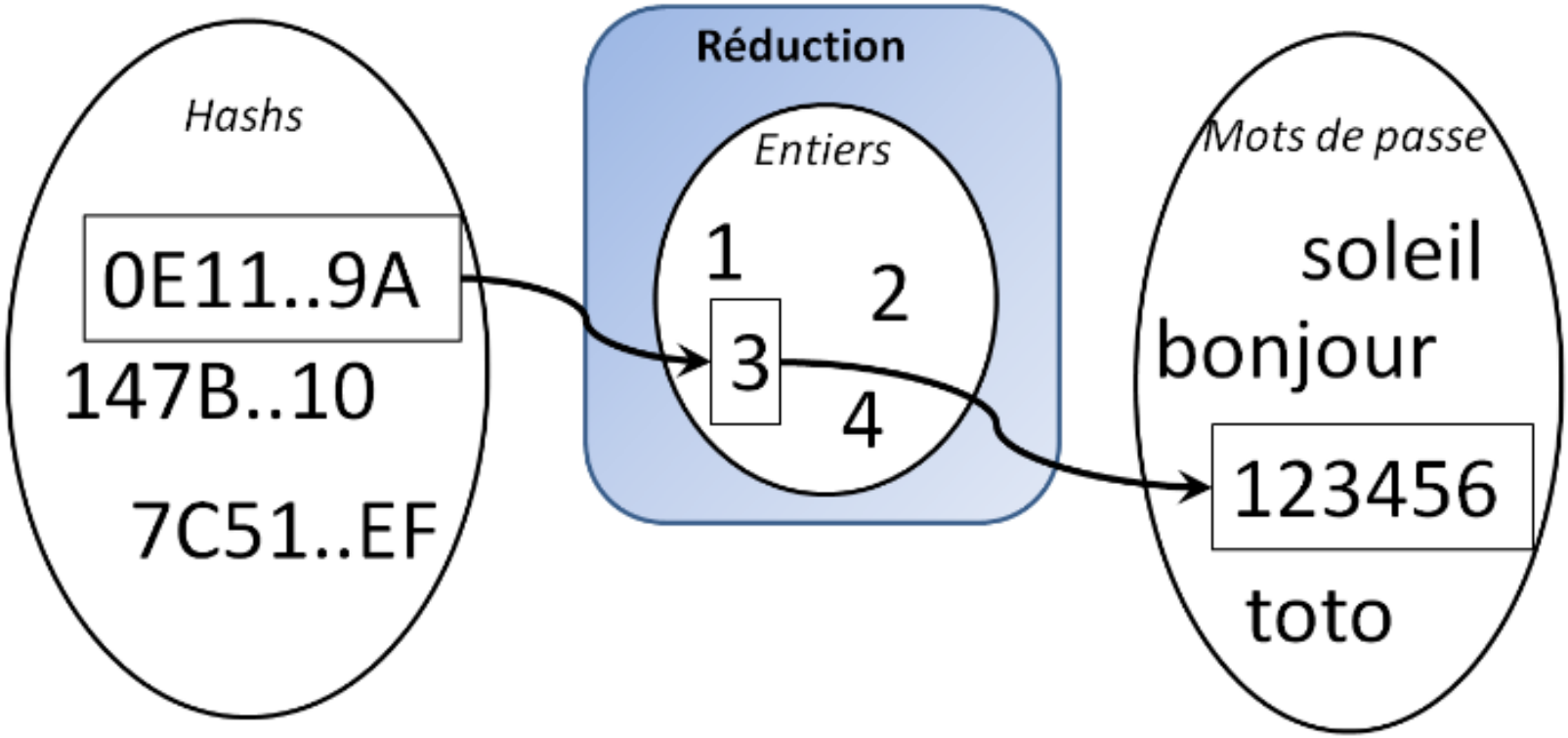


Figure – Décomposition d'une fonction de réduction

Fonctionnalités

Interface graphique

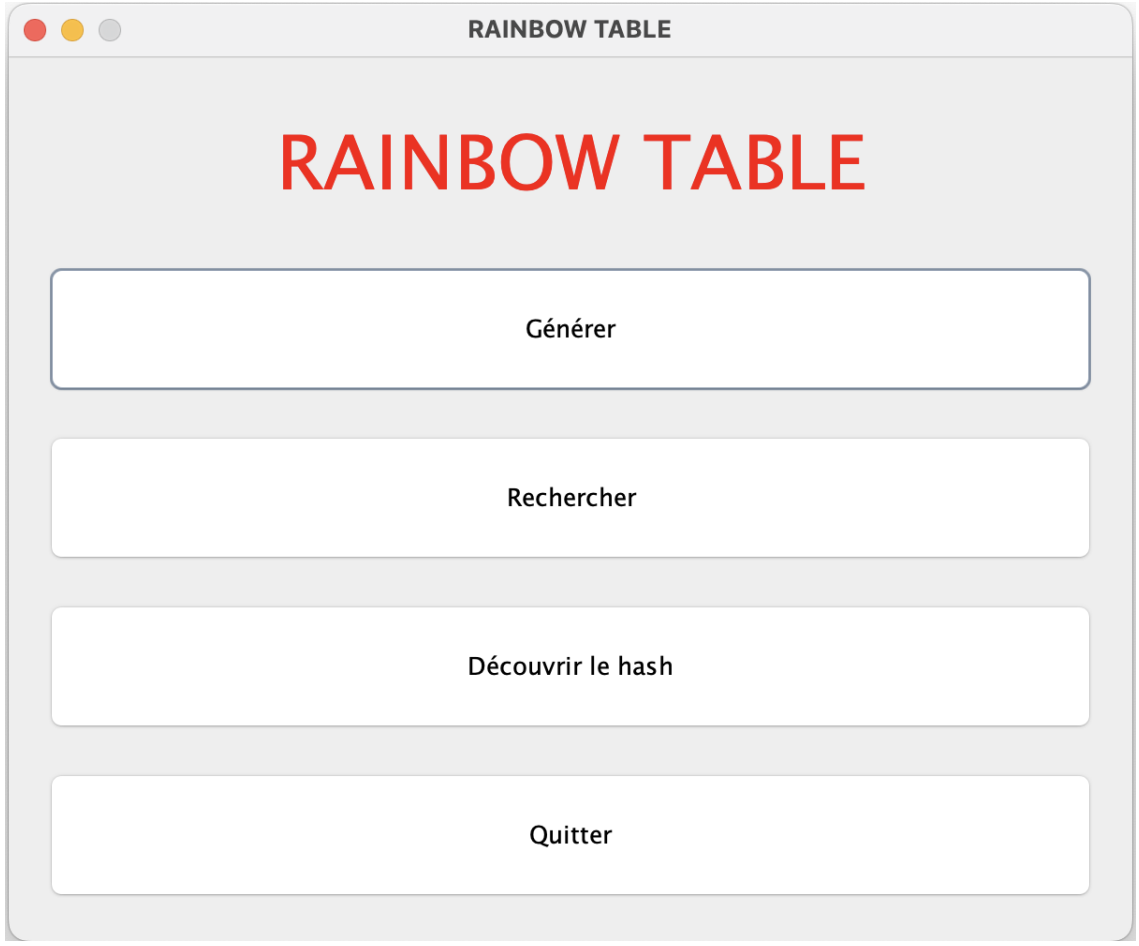


Figure – Interface graphique

*Cette capture d'écran provient de la version mac

Fonctionnalités

Découvrir le hash

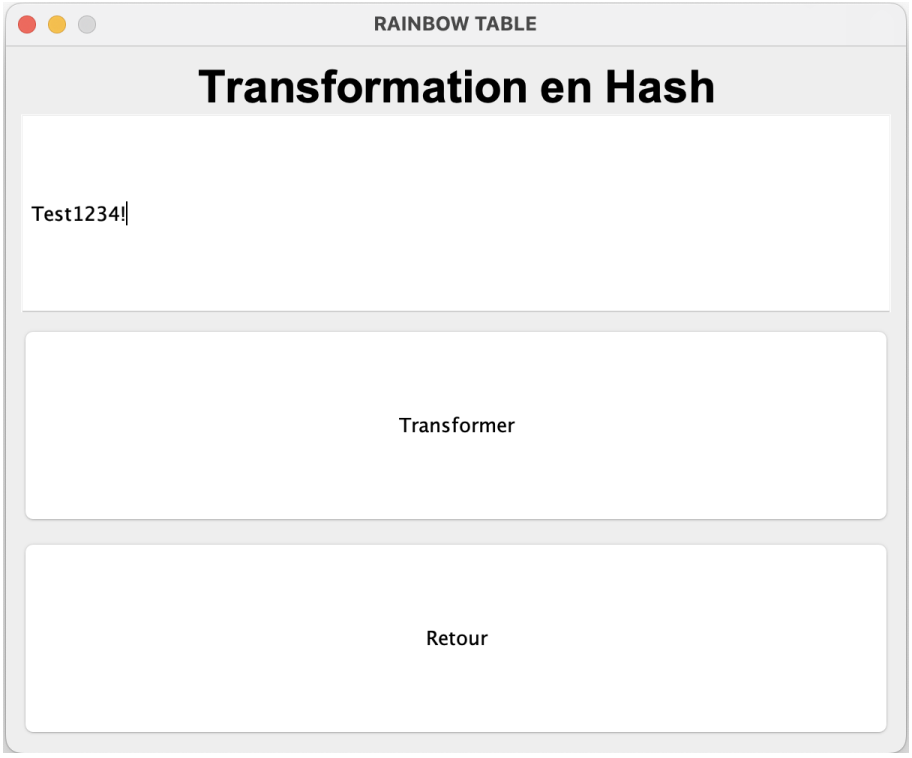


Figure – Mot de passe

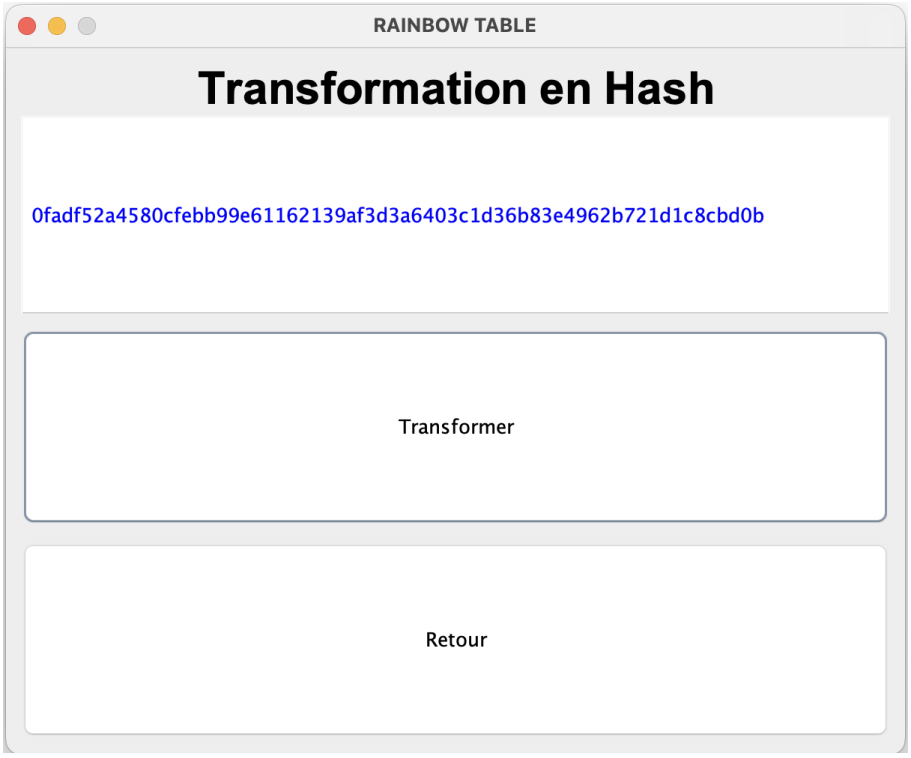


Figure – Hash du mot de passe

*Ces captures d'écran proviennent de la version mac

Fonctionnalités

Découvrir le hash

Pourquoi ces choix ?

⇒ Plus de lisibilité :

- Hash plus reconnaissable
- Meilleure compréhension des fonctionnalités de cette page

⇒ Plus de praticité :

- Possibilité de copier coller directement dans la cellule
- Retour au menu plus rapide

Éléments techniques

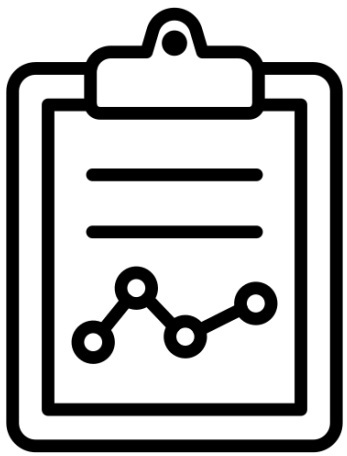
La protection

Comment se protéger des rainbow tables ?

Expérimentations

Résultats quantifiables

Efficacité de la table en fonction des paramètres ?



Expérimentations

Résultats quantifiables

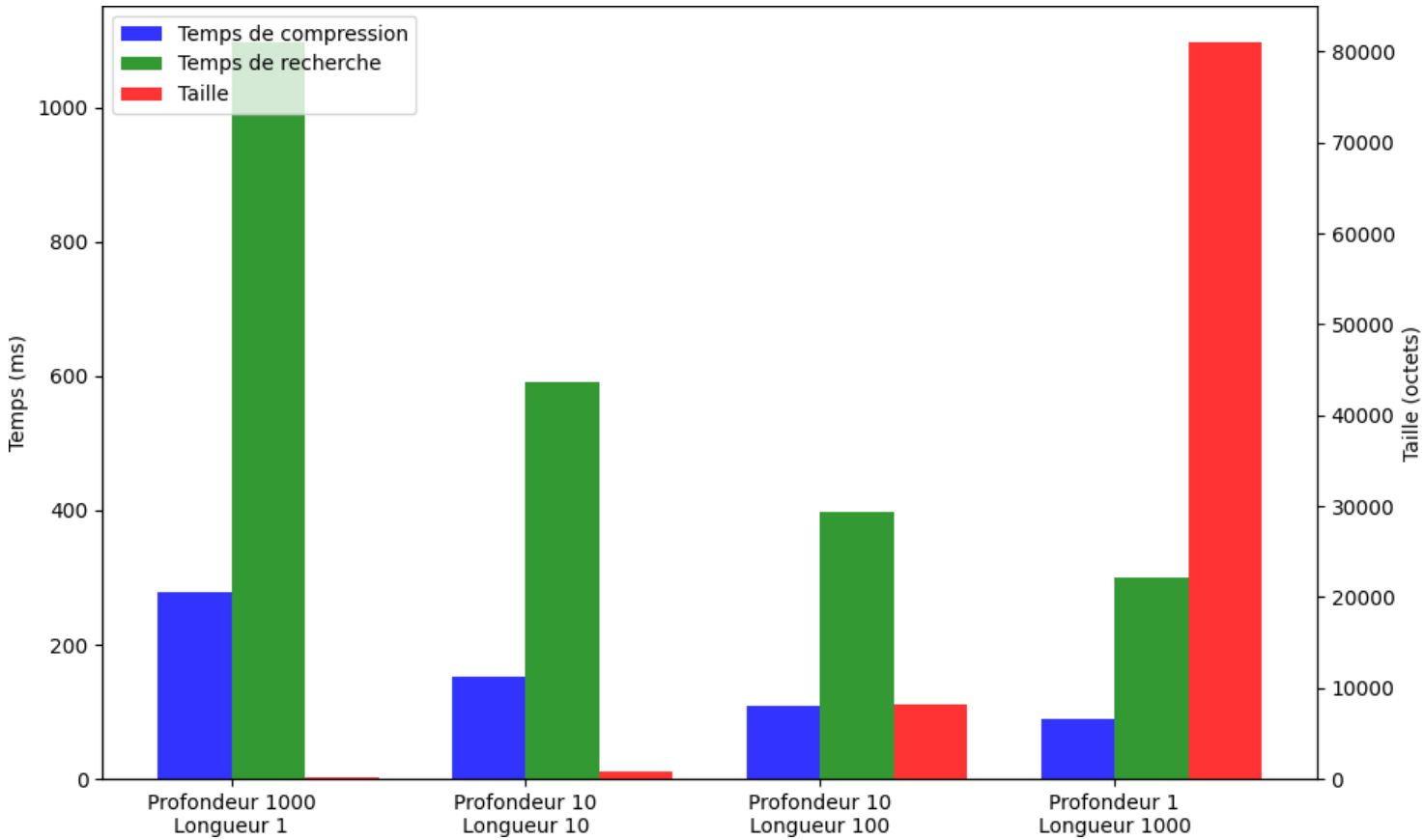


Figure – Graphique représentant le temps de compression, de recherche et la taille en fonction de la profondeur et de la longueur

Conclusion

Avantages et inconvénients

Avantages :

- Rapidité de recherche.

Inconvénients :

- Taille de stockage importante.
- Utilisation limitée pour les mots de passe forts.
- Besoin de mises à jour constantes.

Conclusion

Propositions d'améliorations

- Nouveaux tests unitaires.
- Implémenter des optimisations connues.
- Système de log.
- Nouveaux algorithmes de hachage.
- Des statistiques sur l'interface.