Master 1 Informatique : Cryptographie

Cassage de mots de passe sous Windows et Linux

COIN Lionel et PÔNE Sébastien

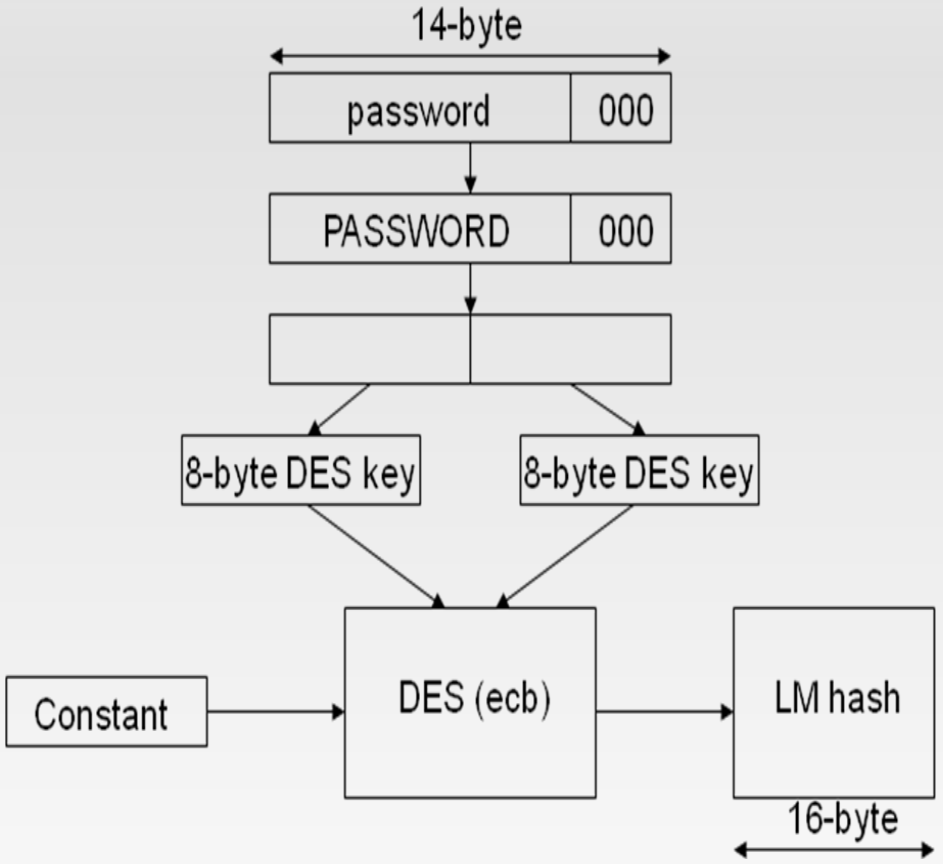
Plan

- Stockage et transformation de mots de passe
  - Système de type Windows
  - Système de type Linux
- Méthodes de cassage de mots de passe
  - Force Brute
  - Dictionnaire
  - Rainbow Table

Stockage et transformation de mots de passe

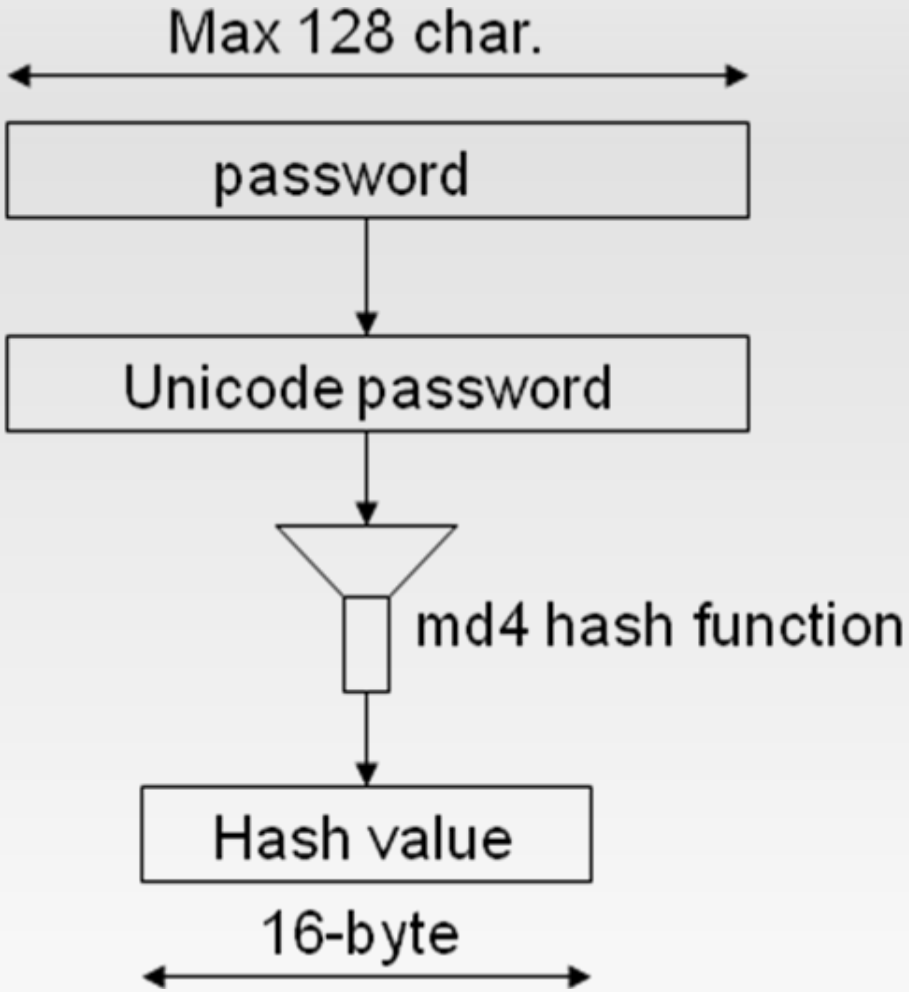
- Pour les systèmes de type Windows, les mots de passe sont stockés dans une partie de la base de registre nommée SAM.
- Stockés sous forme d'empreintes dans le fichier $windir$\system32\config\sam.
- Les empreintes sont obscursies par du chiffrement en utilisant l’algorithme DES.

Algorithmes de hachage pour Windows : LanMan



- Limitation du mot de passe pris en compte à 14 caractères.
- Indifférenciation entre minuscules et majuscules.
- Restriction du nombre de caractères spéciaux/
- Coupure du mot de passe en 2 mots.
- Unicité de l'empreinte pour un même mot de passe.
- Empreinte à 16 caractères.

Algorithmes de hachage pour Windows : NTLM



- Limitation du mot de passe pris en compte à 128 caractères.
- Différenciation entre les minuscules et majuscules.
- Restriction limitée du nombre de caractères spéciaux
- Transformation du mot de passe en Unicode.
- Unicité de l'empreinte par même mot de passe.
- Empreinte à 16 caractères.

Stockage et transformation de mots de passe (2)

- Dans les systèmes Linux, le stockage se faisait sur /etc/passwd mais les mots de passe y sont accessibles à tous
- Les mots de passe sont donc stockés dans /etc/shadow, emplacement accessible uniquement par les administrateurs

Algorithmes de hachage pour Linux

- DES
- MD5
- BlowFish

Attaque par force brute

- Consiste à tester toutes les combinaisons possibles les unes après les autres de façon exhaustive.
- On parcourt toutes les combinaisons de caractères possibles de façon aléatoire pour duper les logiciels de detection d'attaques
- On compare ensuite l'empreinte obtenue avec l'empreinte du mot de passe recherché
- Avantages
  - Le mot de passe est sur d'être trouvé
- Inconvénients
  - Lenteur du procédé
  - Dépend fortement de la puissance de la machine

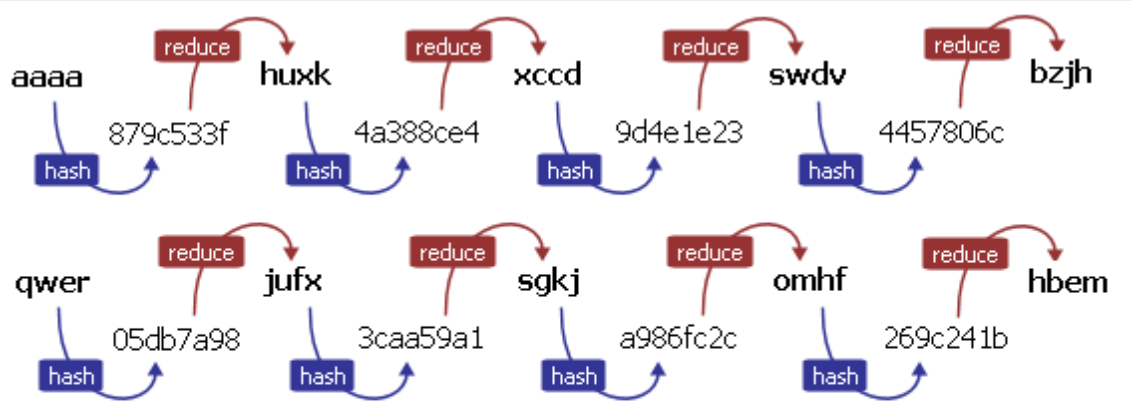
Attaque par dictionnaire

- Consiste à créer une base de données contenant des couples de mot de passe avec leur empreinte puis de les comparer un à un
- Plus le nombre de mots contenus dans la table est important, plus on a de chances de découvrir le mot.
- Avantages
  - Efficace si le mot est dans la base
  - Plus rapide que la méthode de force brute
- Inconvénients
  - Totalement inefficace si le mot n'est pas dans la base
  - Taille du dictionnaire
  - Toujours assez lent

Attaque par Rainbow Table

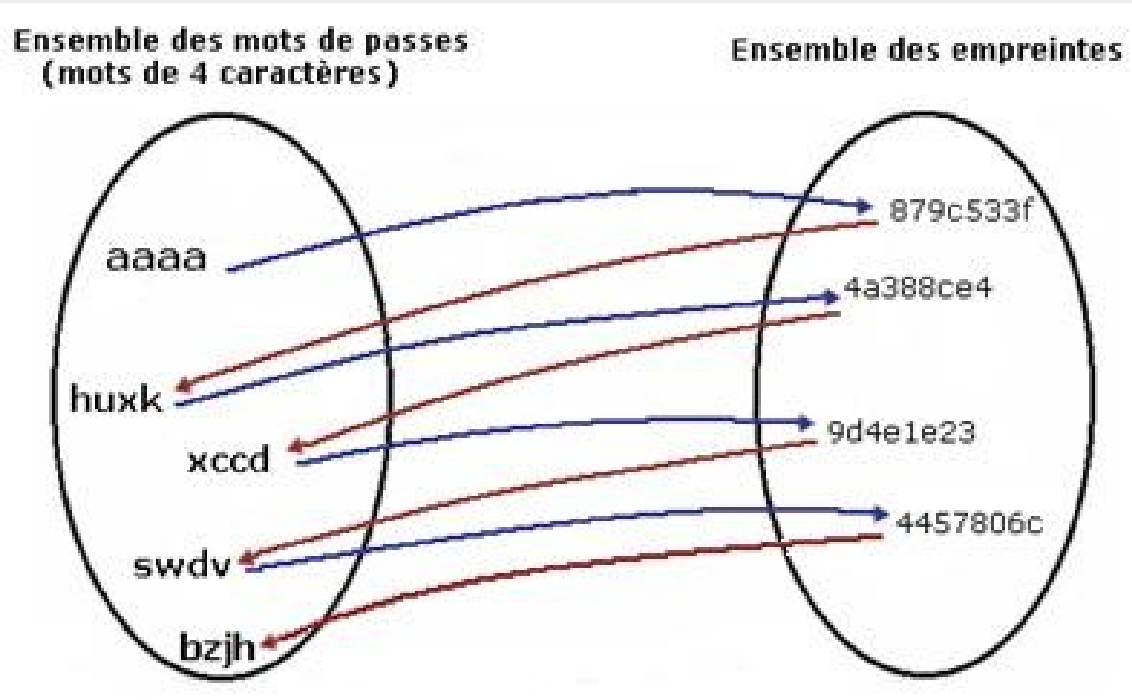
- Création d'une base de donnée d'empreintes/mots de passe
- Optimisation de la base
- Avantages
  - Compromis temps/espace de stockage
- Inconvénients
  - Pas de résultats sûrs à 100%

Construction d'une Rainbow Table

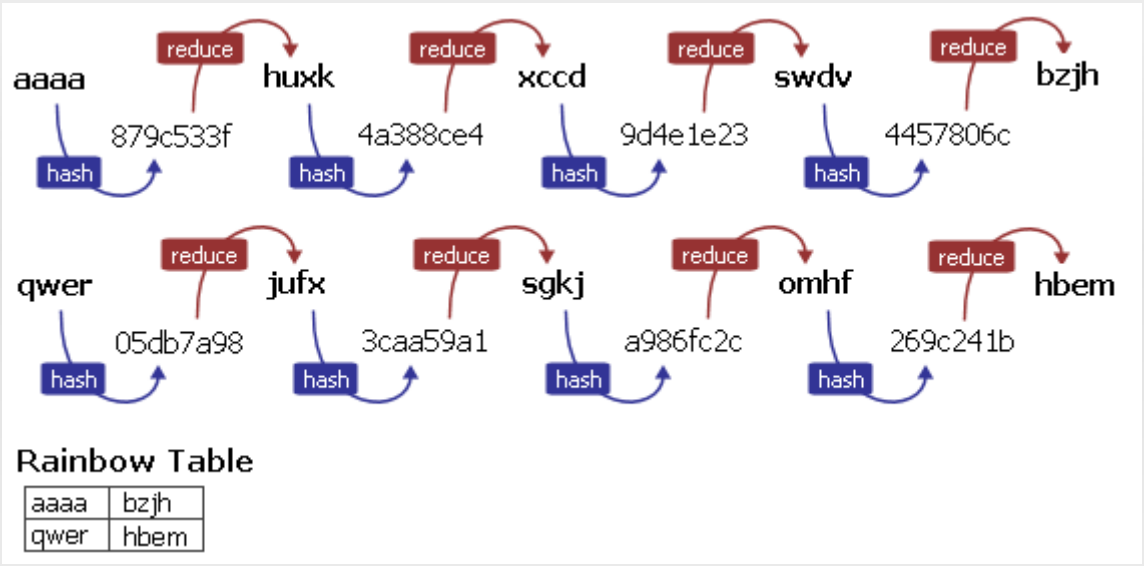


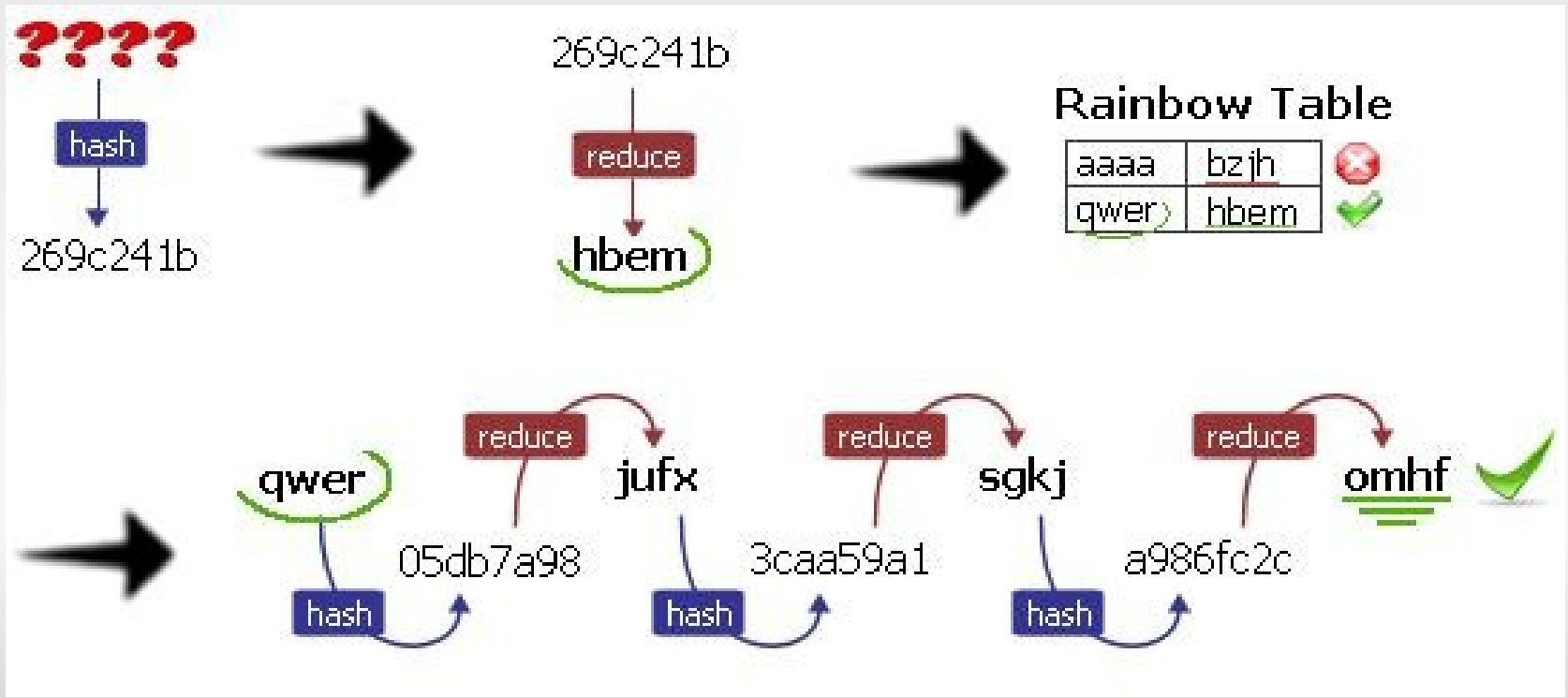
Rainbow Table

aaaa	bzjh
qwer	hbem

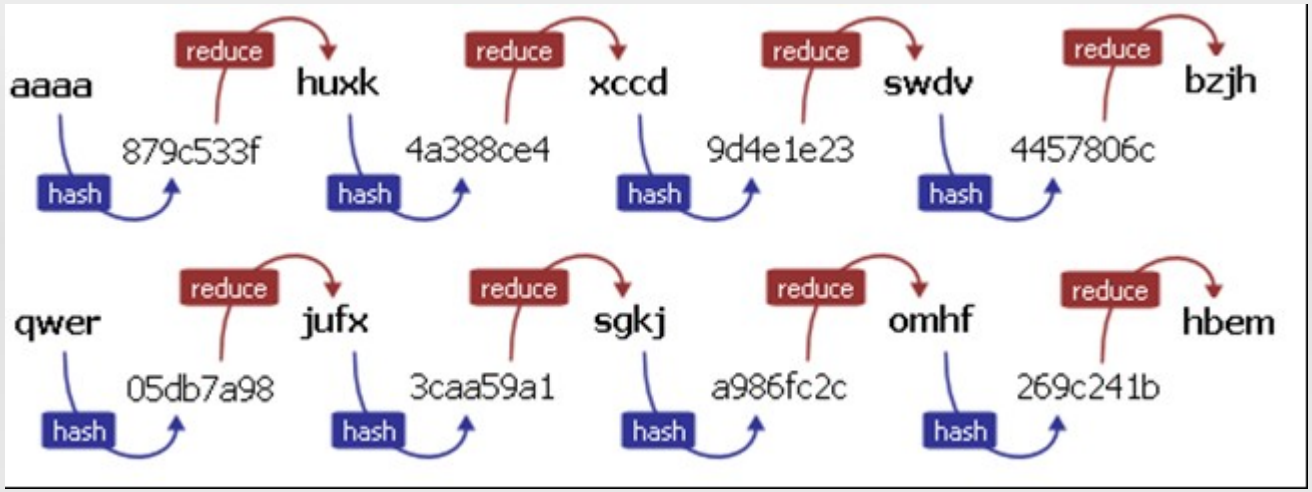


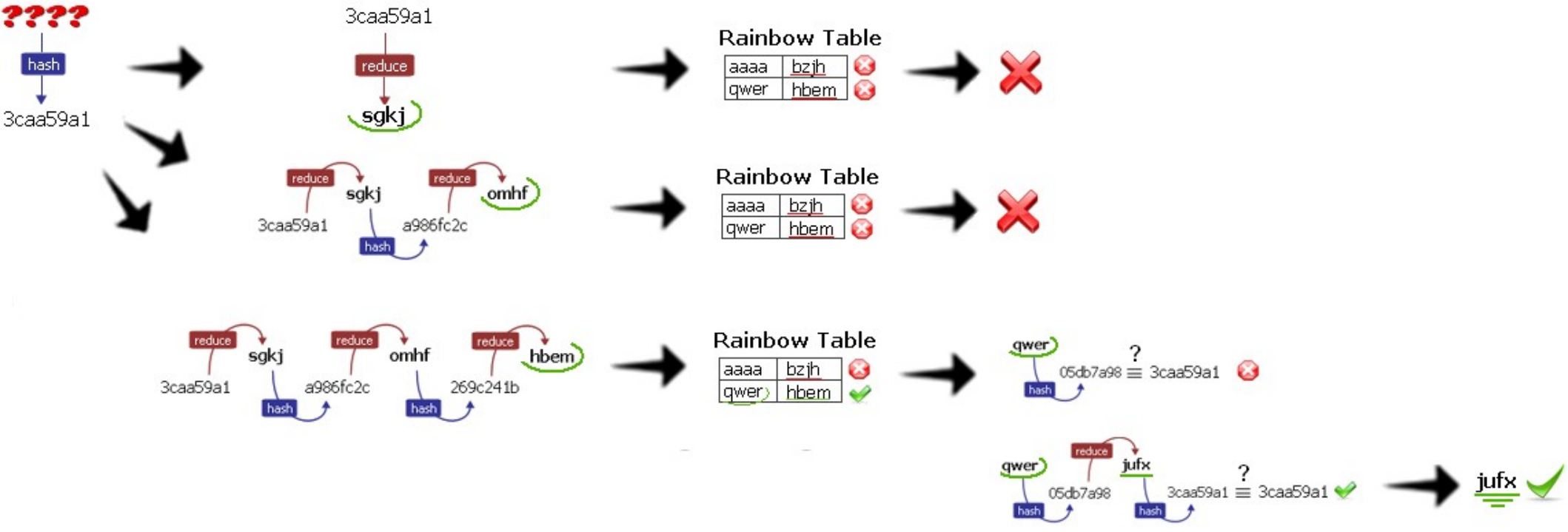
Comparaison – 1er cas



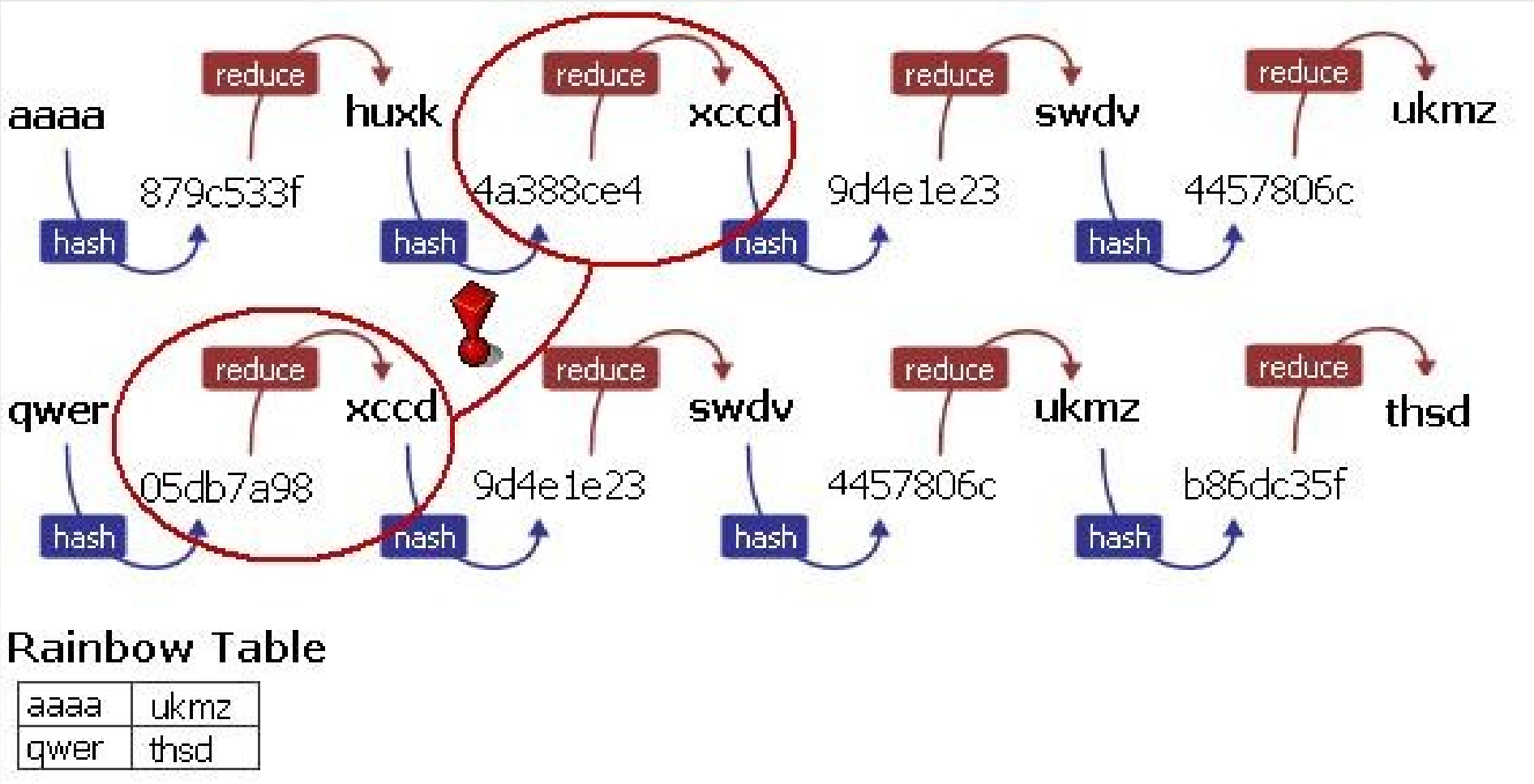


Comparaison – 2eme cas





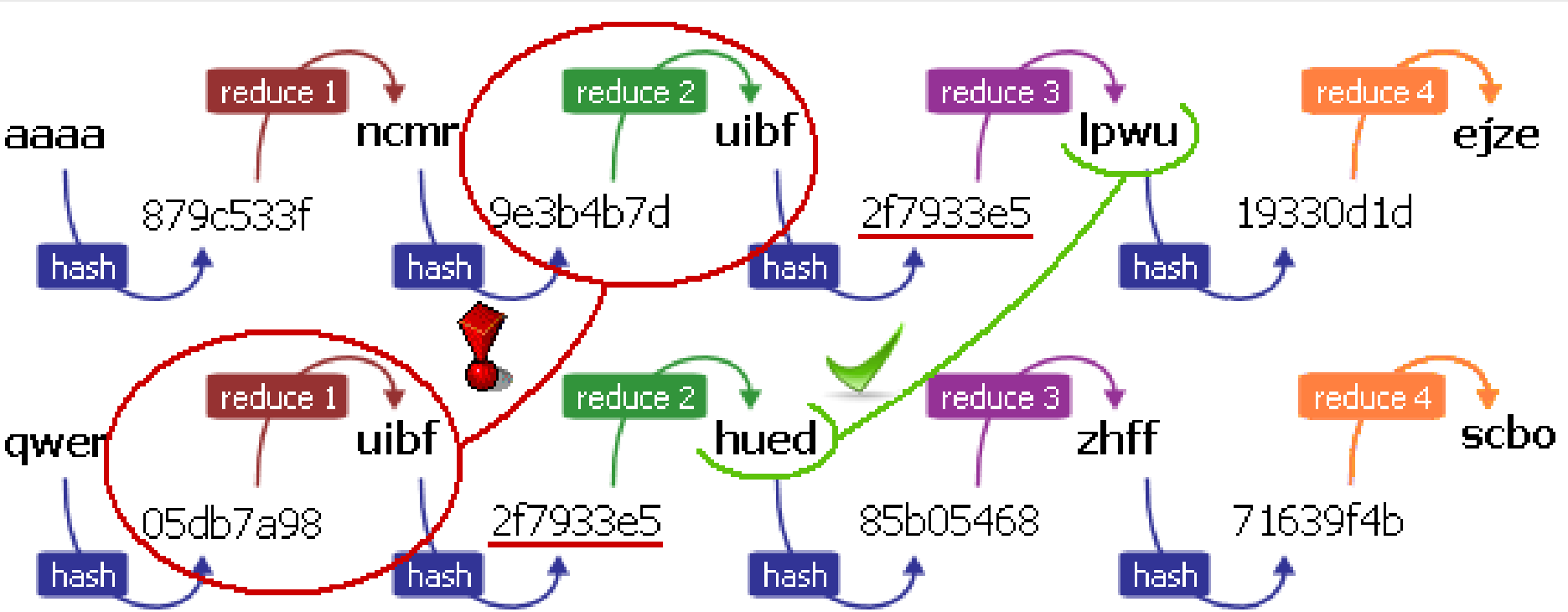
Problème des collisions



Rainbow Table

aaaa	ukmz
qwer	thsd

Problème des collisions : la solution



Rainbow Table

aaaa	ejze
qwer	scbo

Conclusion

- Un mot de passe peut toujours être trouvé et cassé
- Pas de solution ”miracle” un bon rapport temps/ mémoire
- Des solutions sont mises en place pour rendre plus difficile le cassage de mot de passe comme le salage par exemple