

Sommaire

► Introduction

Complexité d'un mot de passe

Rainbow Tables

Rainbow Tables probabilistes

Éléments de performance

Contre-mesures

Questions ?

Introduction

- Pourquoi casser des hashes ?
 - Pentest :
 - > Ré-utilisation dans un contexte différent
 - > Déduction d'autres mots de passe similaires
 - > Agrémenter les rapports
 - Auditer les mots de passe de ses propres utilisateurs
- Comment casser des hashes ?
 - Inverser la fonction de hachage : bonne chance
 - Attaque par force brute : possible sur les mots de passe faibles

Sommaire

Introduction

► **Complexité d'un mot de passe**

Rainbow Tables

Rainbow Tables probabilistes

Éléments de performance

Contre-mesures

Questions ?

Complexité d'un mot de passe

- Qu'est ce qu'un mot de passe faible ?

- > Un mot de passe trop court

toto Jour2 k@!r6

secret Soleil Vo5j.

- > Un mot de passe dérivé de dictionnaire

soleil Bonjour123 SSTIC2011

Bretagne Rennes35 P@ssw0rd

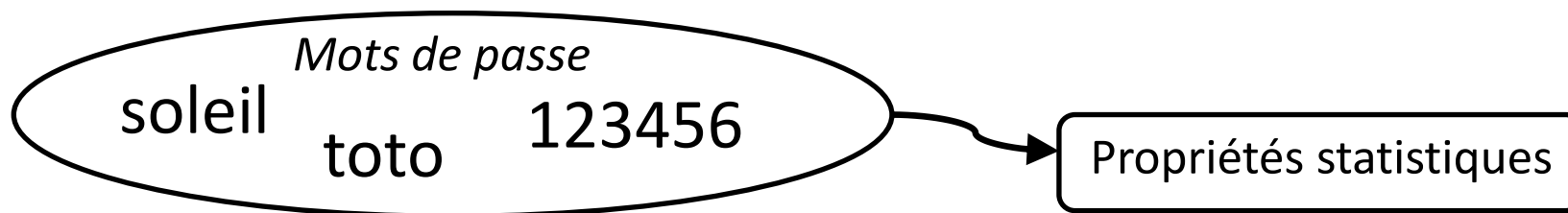
- > Un mot de passe statistiquement probable

SanderS@11 atOM67!!!! Yo101Mama101

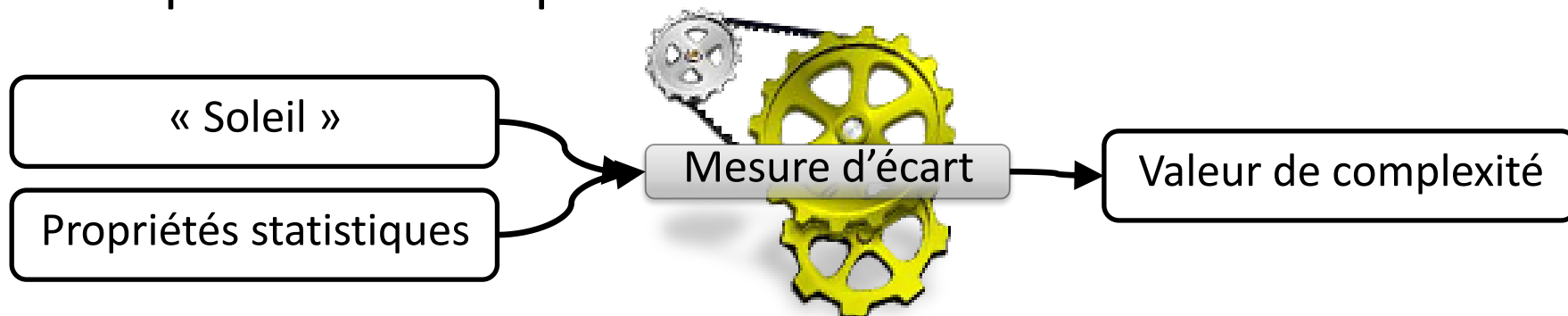
passwot=rd BR@vo1119 @\$H0le123

Complexité d'un mot de passe

- Pour définir la complexité statistique d'un mot de passe on commence par sélectionner un ensemble de mots de passe témoins, puis on en extrait des propriétés statistiques.

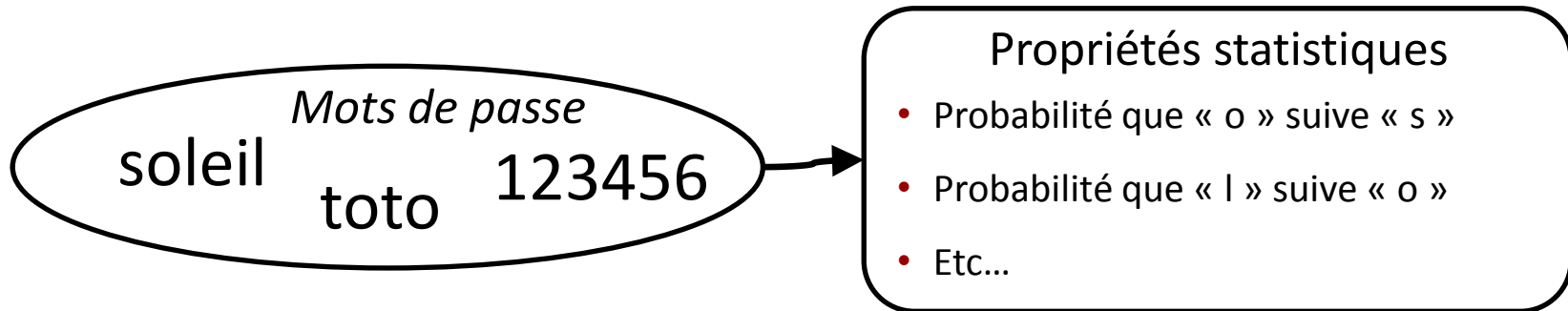


- On mesure ensuite l'écart entre les propriétés statistiques extraites et le mot de passe dont on veut mesurer la complexité statistique



Complexité d'un mot de passe

- L'approche « de Markov », implémenté dans un patch pour John The Ripper :
 - utilise comme propriétés statistiques la probabilité de transition d'une lettre de l'alphabet à une autre :



- base sa mesure d'écart sur le produit des probabilité de toutes les transitions d'un mot :

$$\text{Mesure}(\ll \text{LOL} \gg) = P('L').P('L' \rightarrow 'O') .P('O' \rightarrow 'L')$$

- Mesure en fait précisément comme ceci :

$$\text{Mesure}(\ll \text{LOL} \gg) = -1000.\log(P('L').P('L' \rightarrow 'O') .P('O' \rightarrow 'L'))$$

Complexité d'un mot de passe

- L'approche « de Markov », donne d'excellents résultats et est aujourd'hui incontournable :
 - Largement utilisée au challenge « Crack me if you can »
- Élément de pertinence :
 - **50%** des mots de passe du site web « RockYou » peuvent être cassés en parcourant les 3 313 285 977 (**3G**) mots de passe ayant une complexité de Markov inférieure au seuil 225.
 - A titre de comparaison les 20 158 268 677 (**20G**) de mots de passe constitués de toutes les combinaisons possible majuscule/minuscule jusqu'à 6 caractères ne retrouvent que **16%** des même mots de passe.

Sommaire

Introduction

Complexité d'un mot de passe

► **Rainbow Tables**

Rainbow Tables probabilistes

Éléments de performance

Contre-mesures

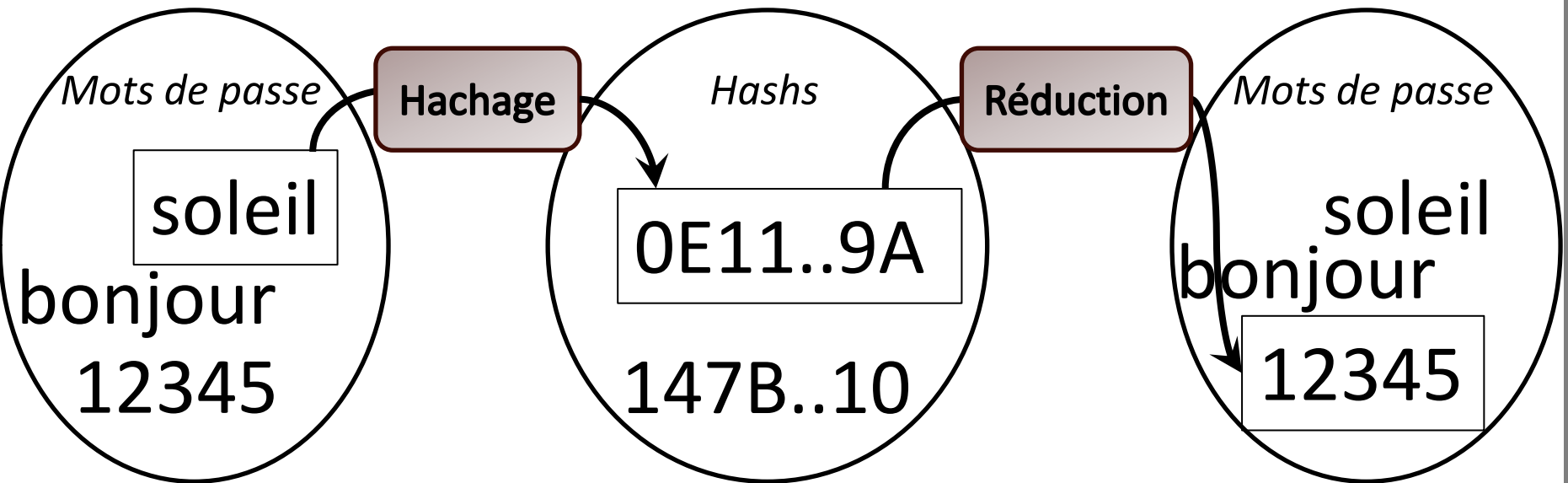
Questions ?

Rainbow Tables

- Les Rainbow Tables permettent de casser des hashes rapidement en mettant en œuvre un compromis temps/mémoire.
- Macroscopiquement la technologie des Rainbow Table se met en œuvre en 2 temps :
 1. Pré-calculer les hashes d'un ensemble de mots, et stocker les association « mot / hash » (de façon efficace) dans une structure appelée « Rainbow Table »
 2. Effectuer une recherche (rapide) dans la « Rainbow Table » afin de retrouver un mot en clair qui donne le hash que l'on cherche à casser (si le hash en question est dans l'une des correspondance pré-calculée)

Rainbow Tables

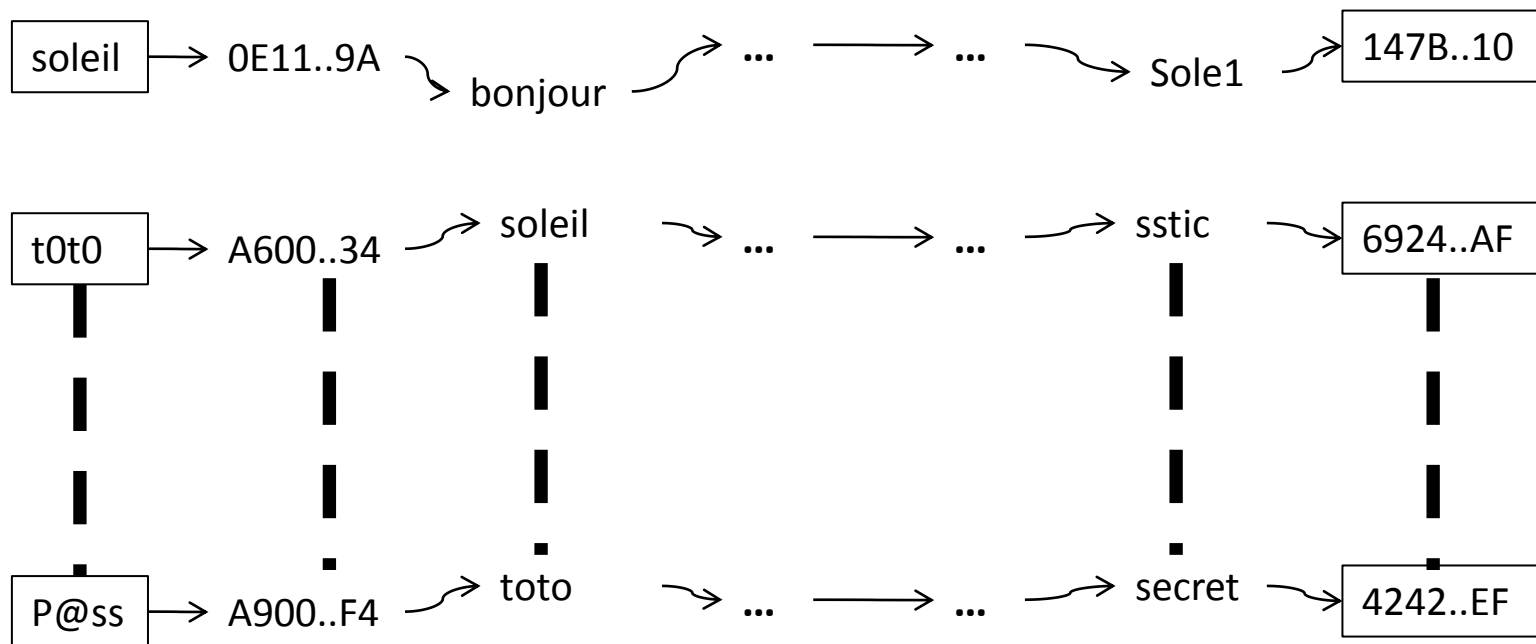
- Construire une Rainbow Table nécessite 3 choses :
 - Un ensemble de mots en clair (mots de passe candidats)
 - Une fonction de hachage (sans commentaire)
 - Une fonction de réduction.



- En itérant le processus « hachage/réduction » plusieurs milliers de fois on génère une « chaine » de mots de passe. Chaque « chaine » contient la mémoire des milliers d'association « mot de passe / hash » qui la compose.

Rainbow Tables

- L'ensemble de nos chaines constitue une Rainbow Table
- On mémorise chaque chaine en stockant uniquement son premier et son dernier élément.



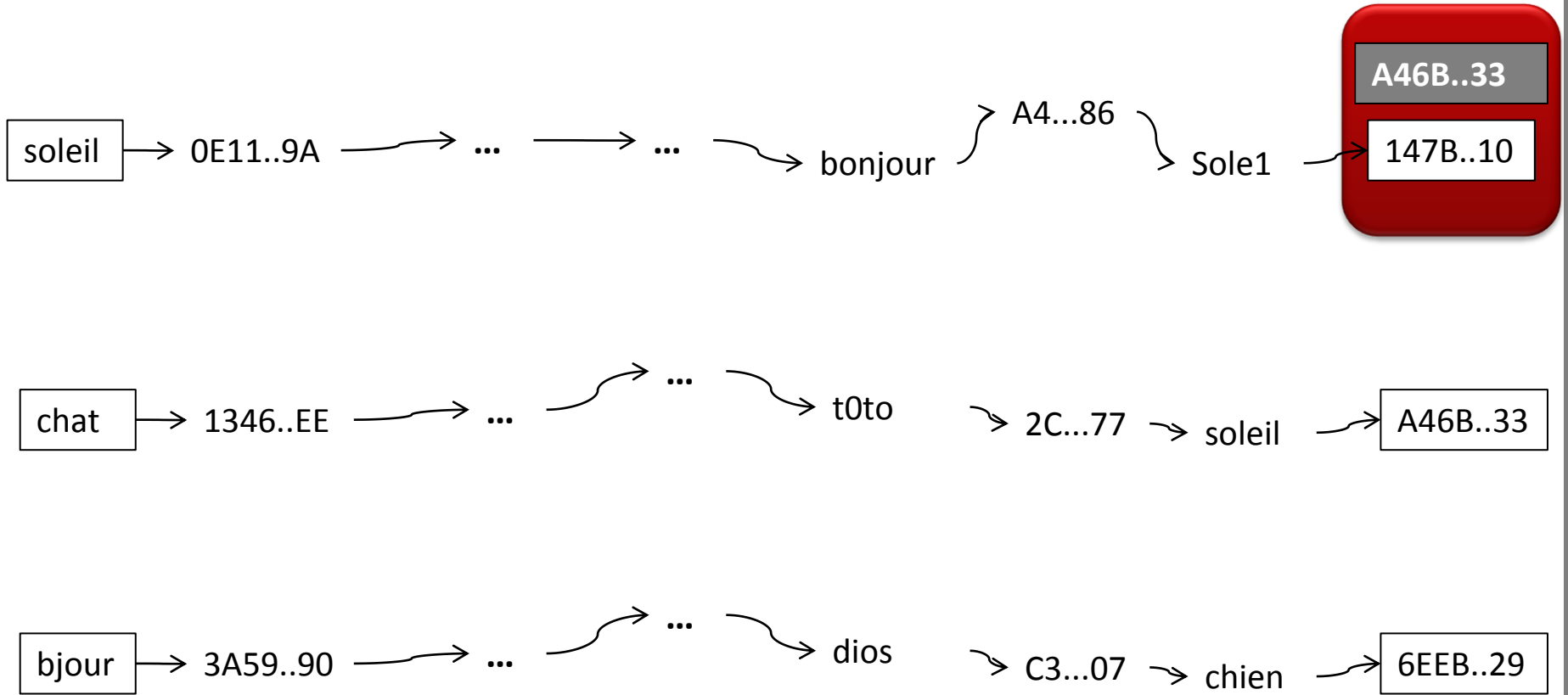
Rainbow Tables

- Recherche dans une Rainbow Table **A46B..33**



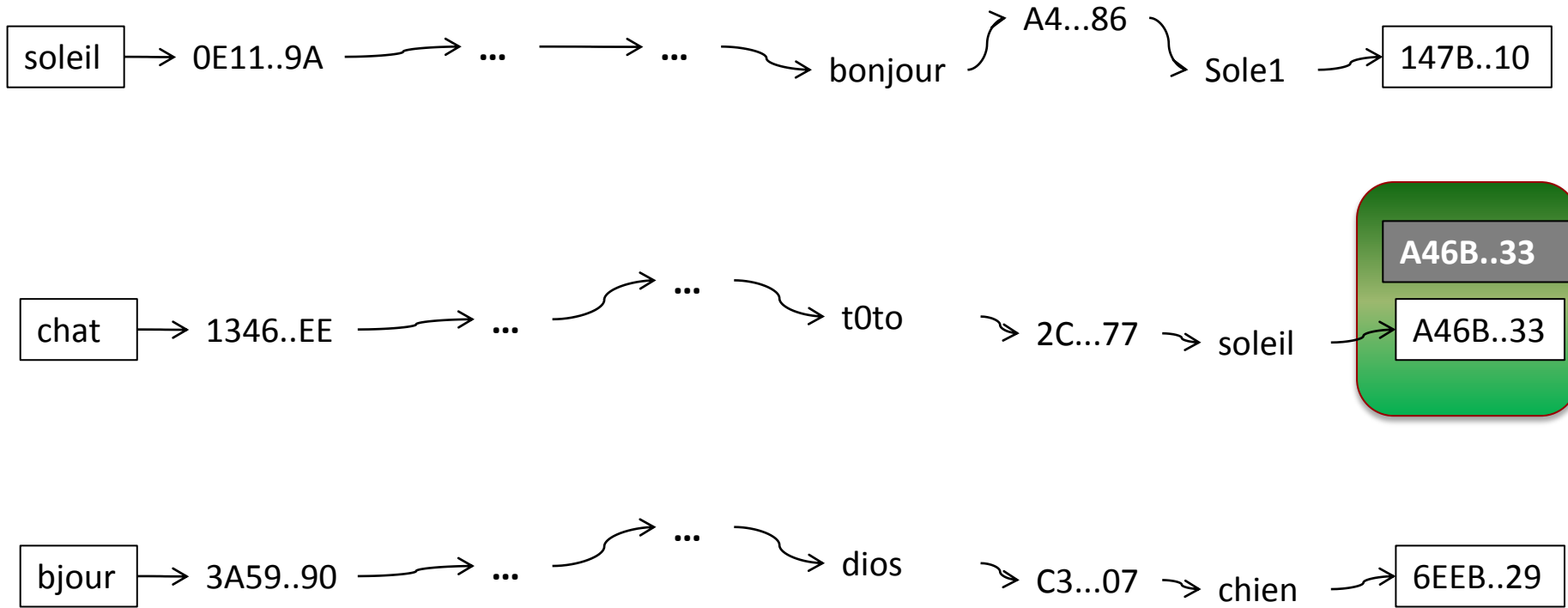
Rainbow Tables

- Recherche dans une Rainbow Table



Rainbow Tables

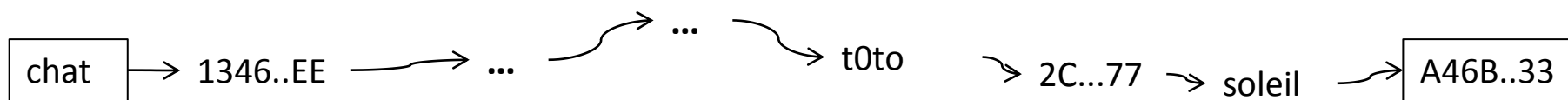
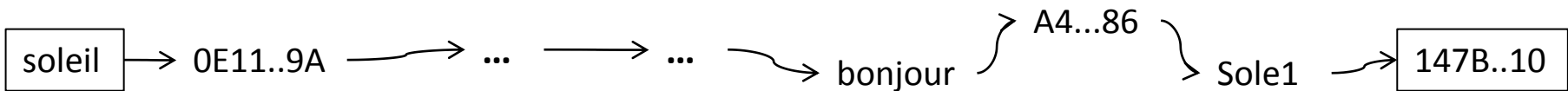
- Recherche dans une Rainbow Table



Rainbow Tables

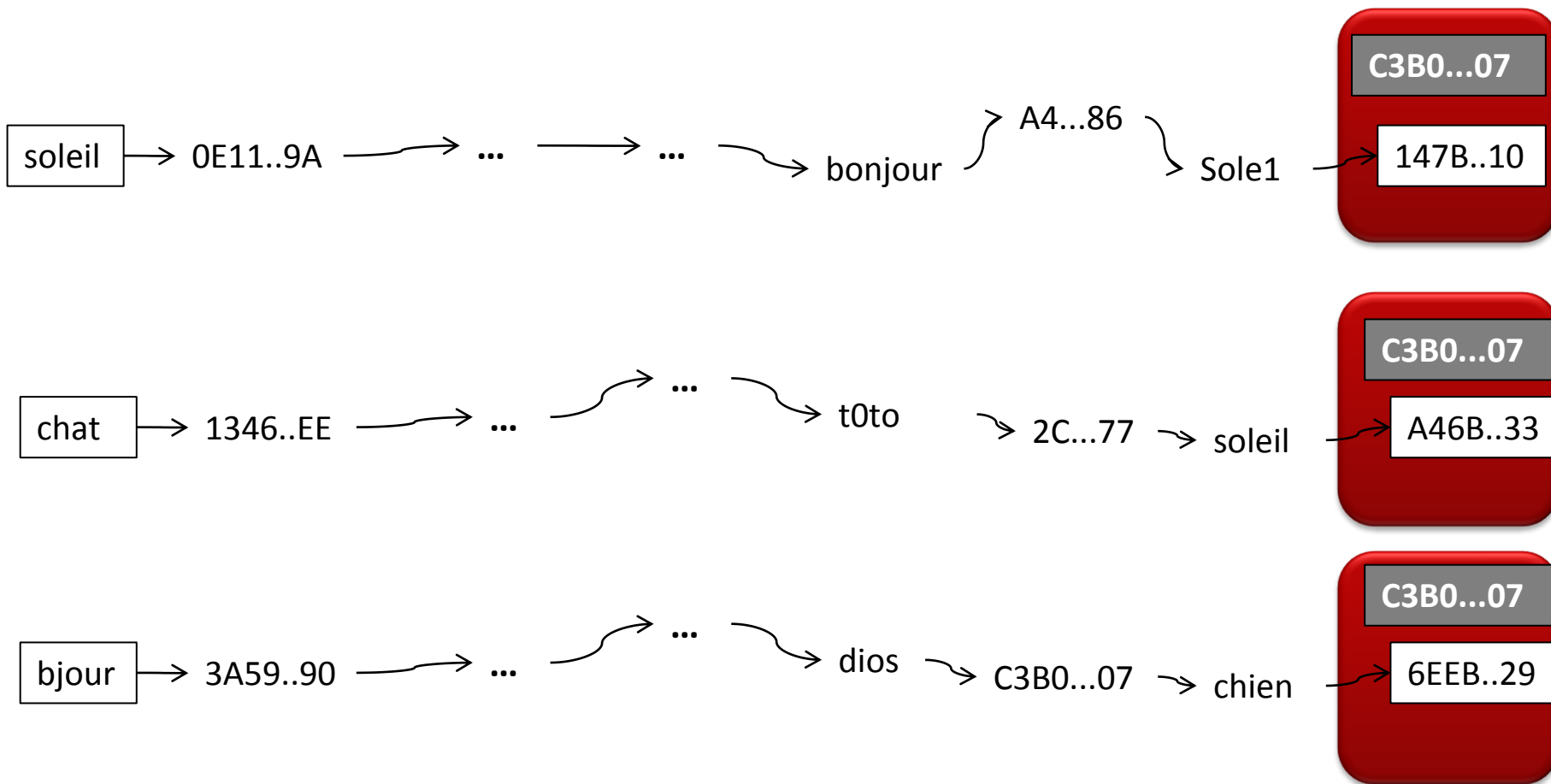
- Recherche dans une Rainbow Table

C3B0...07



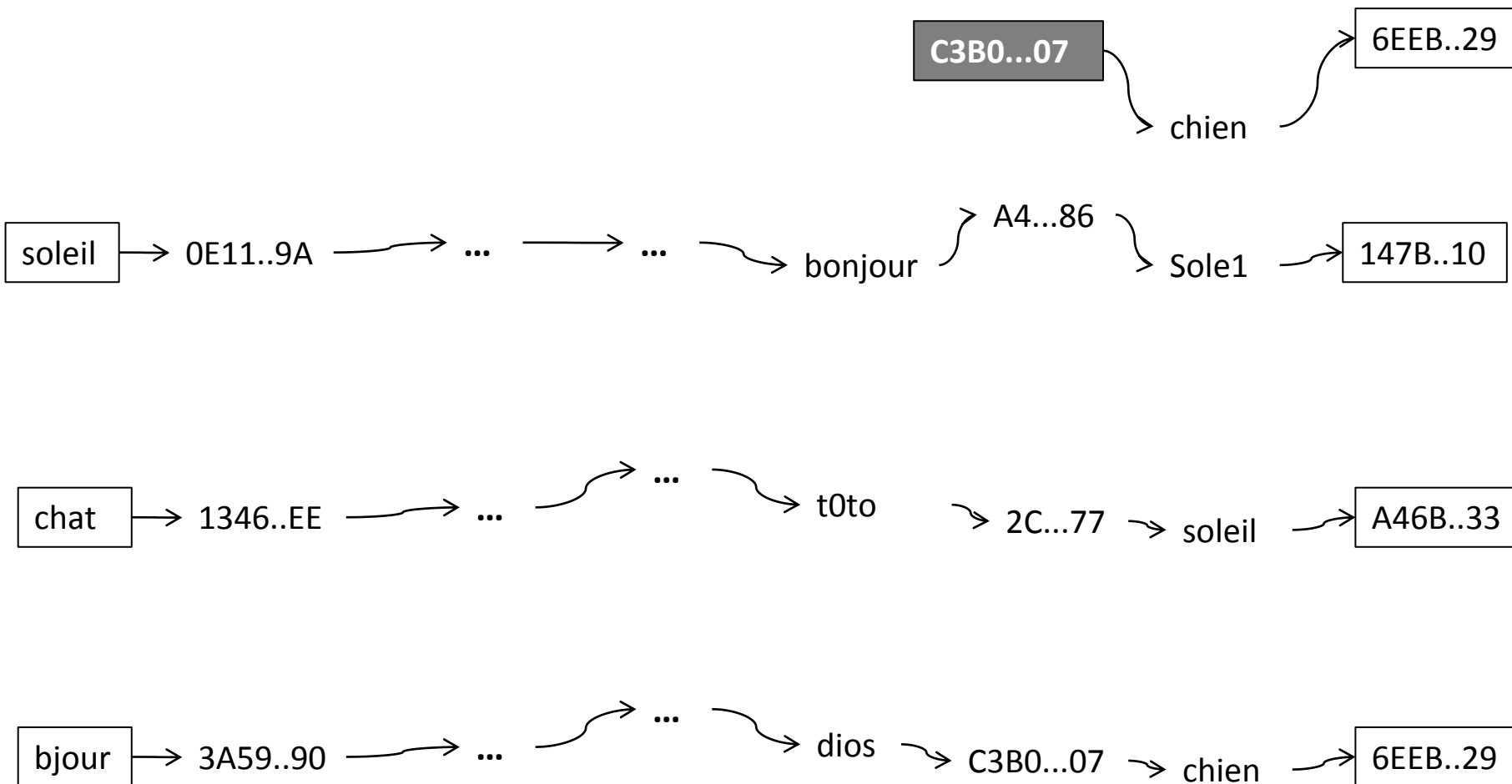
Rainbow Tables

- Recherche dans une Rainbow Table



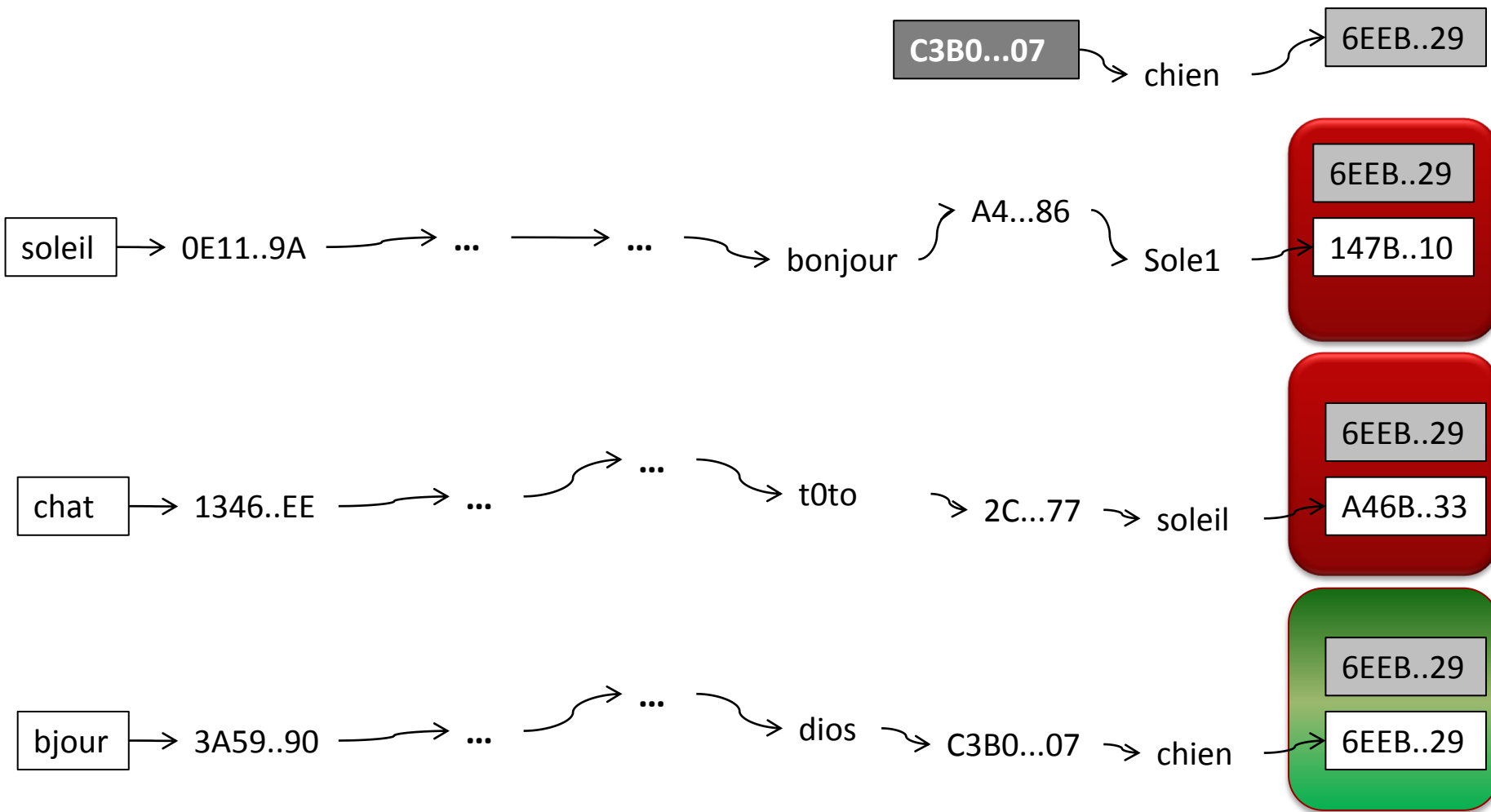
Rainbow Tables

- Recherche dans une Rainbow Table



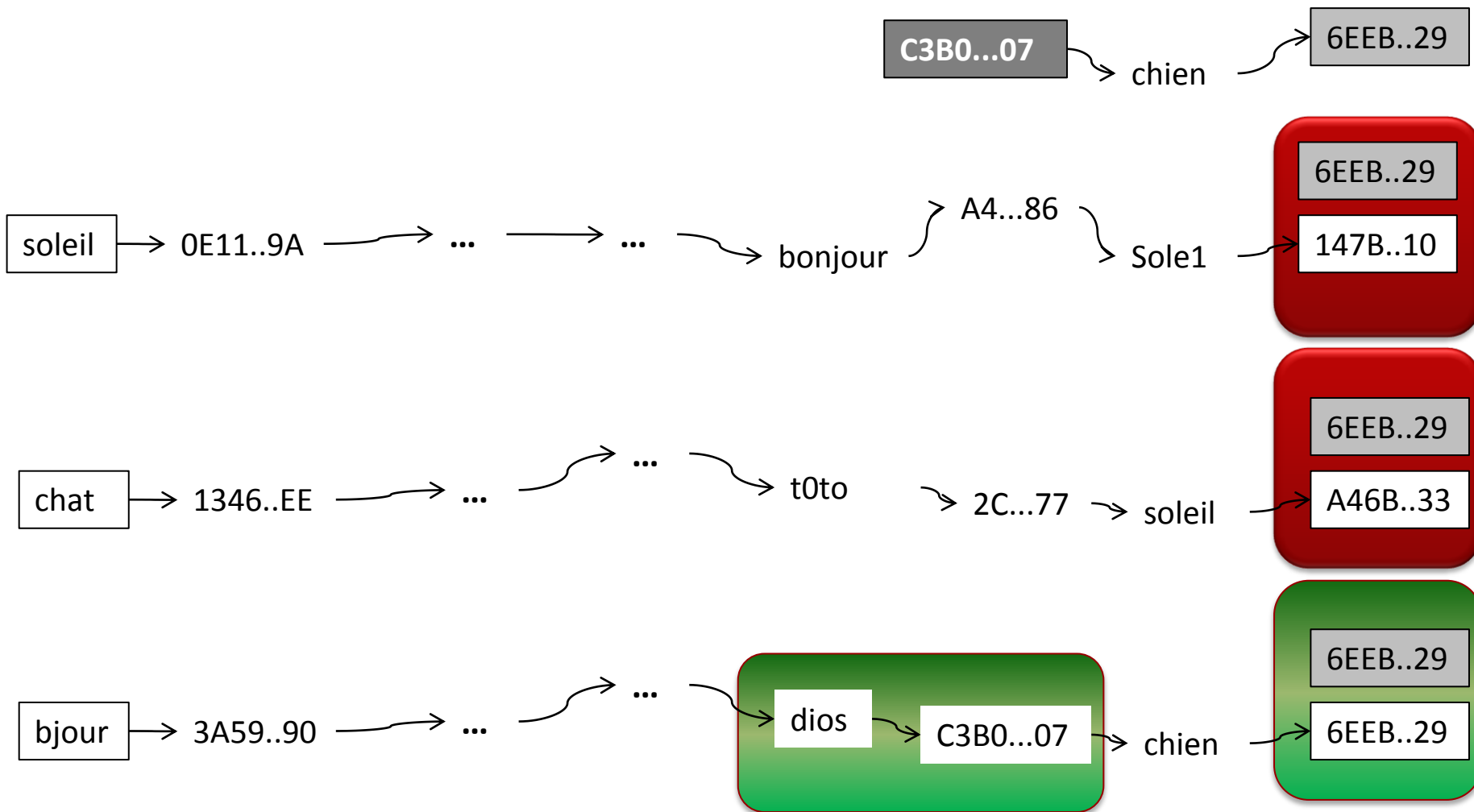
Rainbow Tables

- Recherche dans une Rainbow Table



Rainbow Tables

- Recherche dans une Rainbow Table



Rainbow Tables

- Compromis temps/mémoire, à quel point est-ce efficace ?
 - LM : virtuellement 100% de succès, en moins d'une minute.
 - NT : les mots de passe de 7 caractères ou moins sont cassés en quelques minutes.
- En moins de quelques instants on réalise donc l'équivalent d'une attaque par force brute sur un ensemble de plusieurs téra mots de passe (~3 500 000 000 000 mixed alphanumeric 1-7). Un PC calculant 30 millions de hashes/seconde aurait besoin d'environ 32h. Imaginez pour « all-chars 1-8 »...

Sommaire

Introduction

Complexité d'un mot de passe

Rainbow Tables

► **Rainbow Tables probabilistes**

Éléments de performance

Contre-mesures

Questions ?

Rainbow Table probabilistes

- La question : Existe-t-il des Rainbow Tables d'espace de Markov ?
- La réponse :
 - Les Rainbow Tables classique énumèrent toutes les combinaisons possibles d'un certain alphabet jusqu'à une certaine longueur.
 - Il existe des Rainbow Tables basées sur des dictionnaires.
 - Il existe des Rainbow Tables hybrides.
 - **Il n'existe pas de Rainbow Tables basées sur des espaces de Markov.**

Rainbow Table probabilistes

- La question : Pourquoi n'existe-t-il pas de Rainbow Tables basées sur des espaces de Markov ?
- Pourtant, pour faire une Rainbow on n'a besoin que de :
 - Une fonction de hachage
 - Une fonction de réduction
 - Un ensemble de mot de passe


Rainbow Table probabilistes

- La question : Pourquoi n'existe-t-il pas de Rainbow Tables basées sur des espaces de Markov ?
- Pourtant, pour faire une Rainbow on n'a besoin que de :
 - Une fonction de hachage
 - Une fonction de réduction
 - Un ensemble de mot de passe **dénombrable et pour lequel on sait rapidement obtenir le N-ième mot de passe pour tout entier N.**

Rainbow Table probabilistes

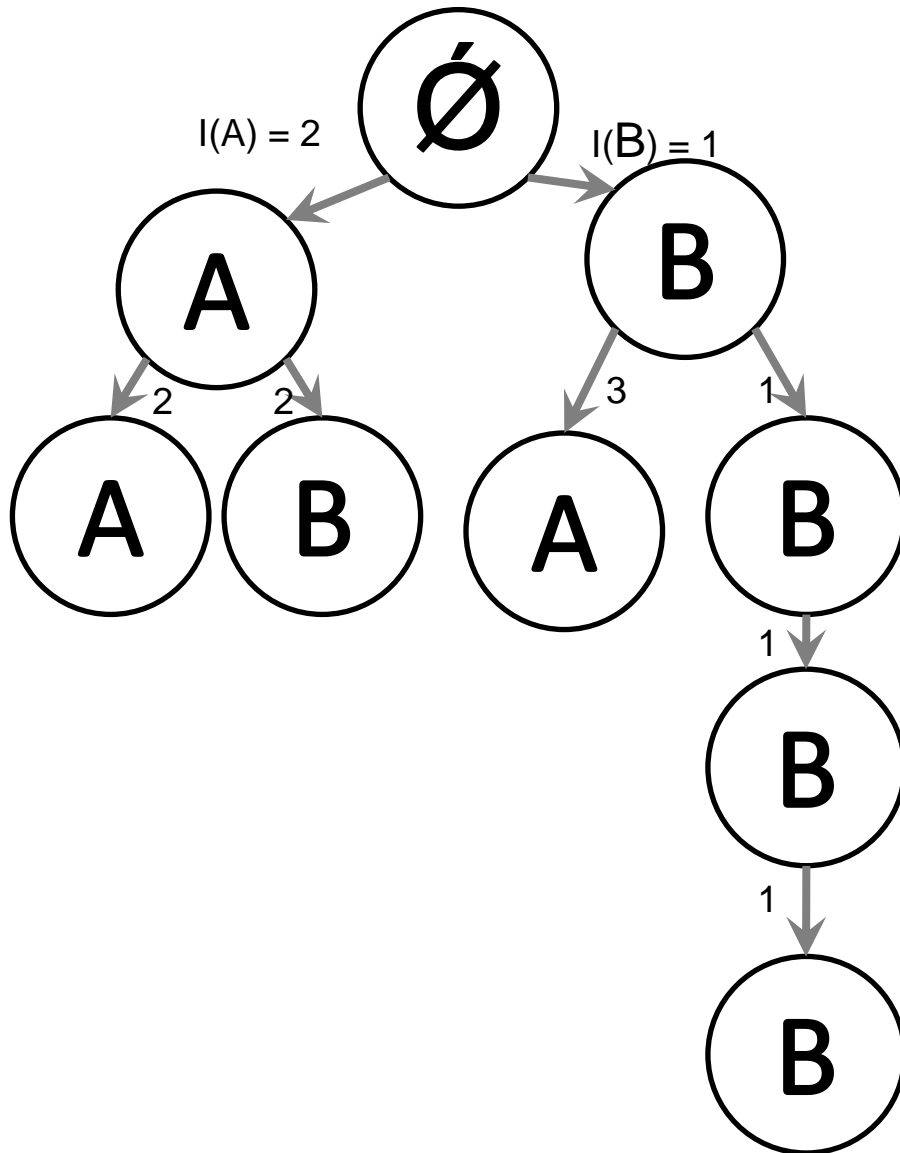
- Comment numéroté nos mots de passe de Markov ?
 - Prenons un alphabet de démonstration, constitué des lettres « A » et « B ».
 - Supposons les propriétés statistiques ci-dessous :

Tableau de complexité

Complexité 	A	B
A	2	2
B	3	1

Rainbow Table probabilistes

- L'espace de Markov de complexité 4 à numéroté est :



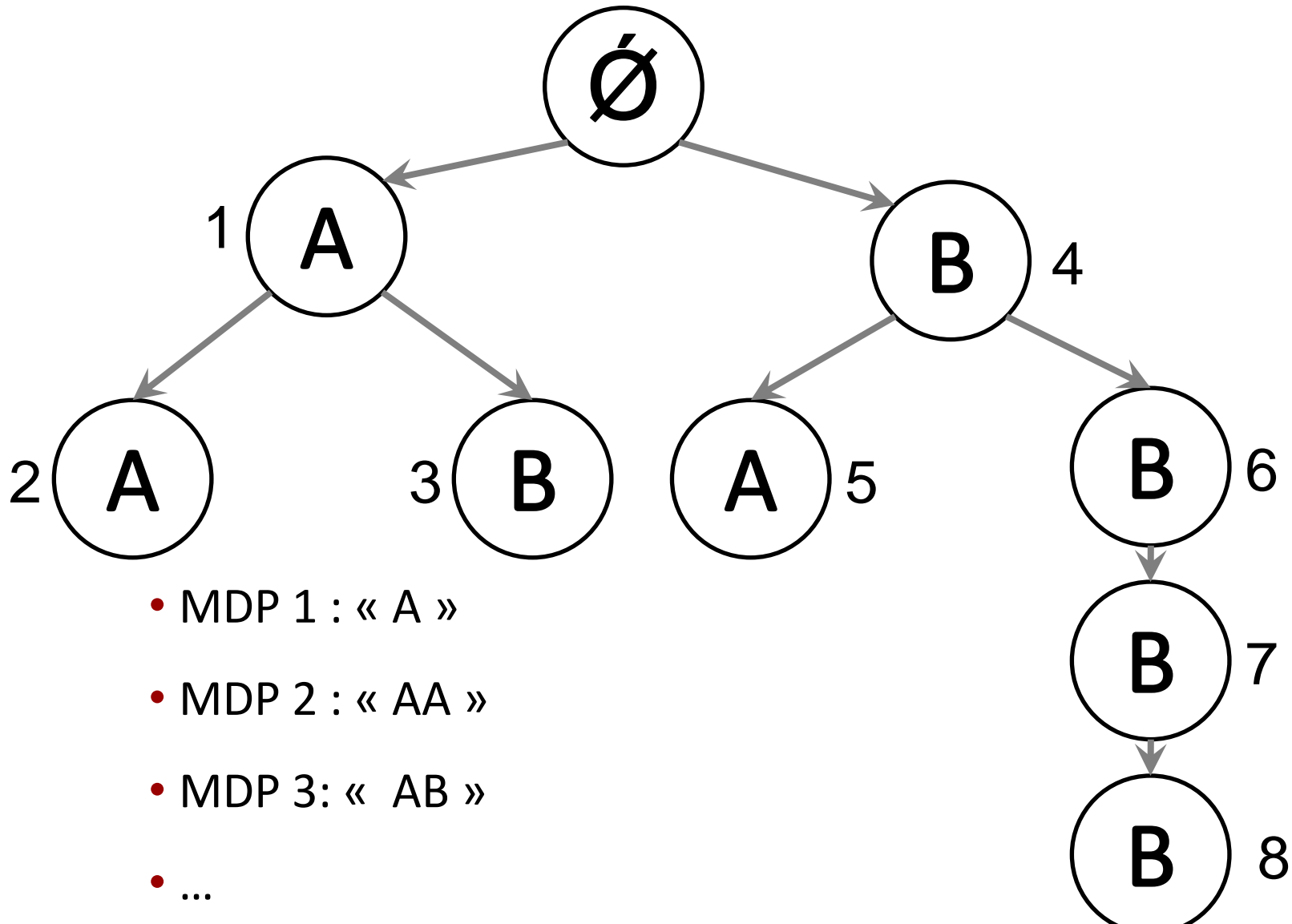
- La construction se fait à partir de la racine, de proche en proche en réduisant petit à petit notre capital de complexité restant.

Tableau de complexité

Complexité	A	B
A	2	2
B	3	1

Rainbow Table probabilistes

- Comment numéroter nos mots de passe de Markov ?



Rainbow Table probabilistes

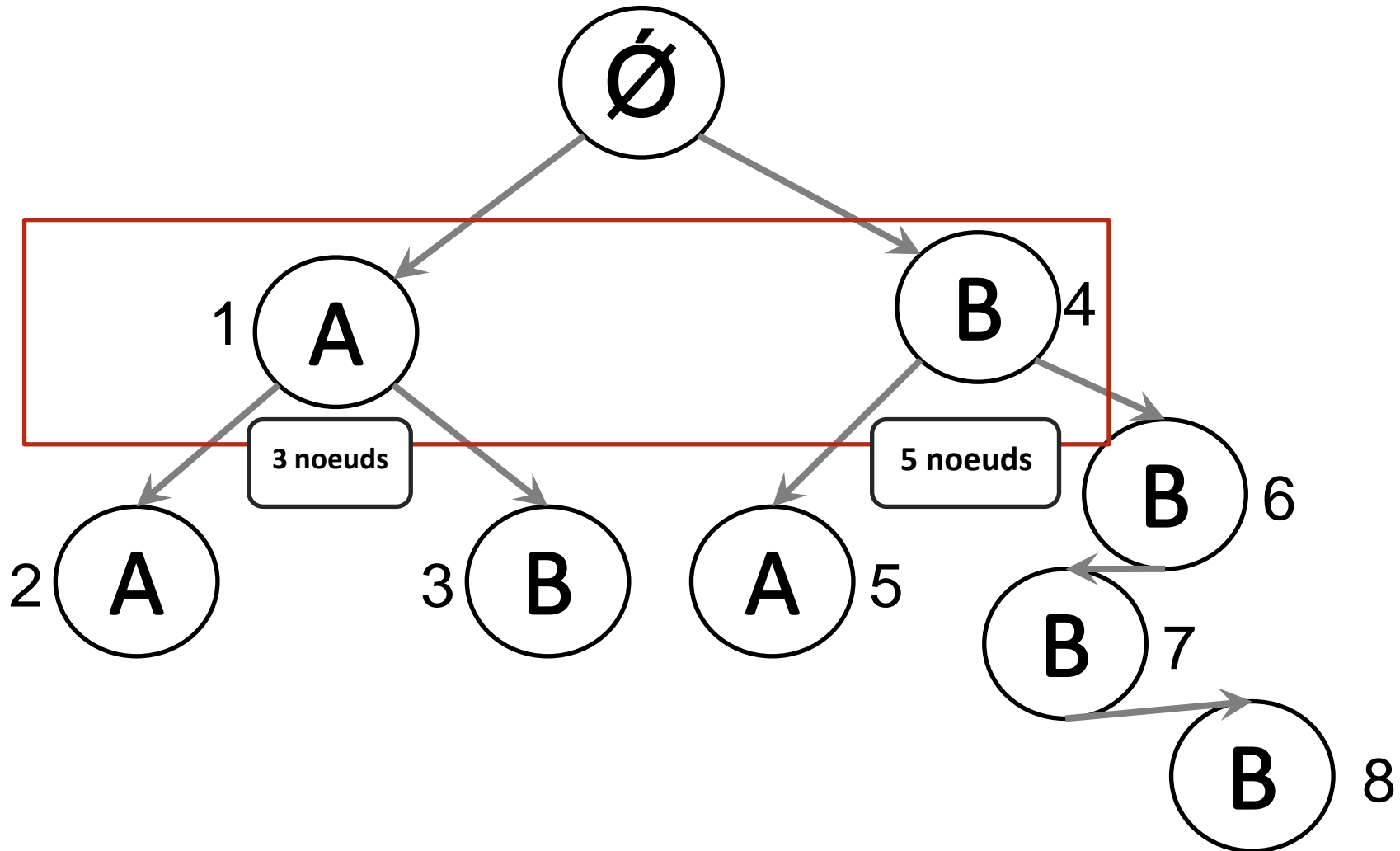
- Problème : accéder au N-ième élément de ce type d'arbre est excessivement lent, et c'est cet accès qui devient limitant par rapport au calcul du hash pour les algorithmes les plus rapides → Il n'est pas intéressant de calculer des Rainbow Tables de Markov....sur CPU
- Et si on essayait de générer nos Rainbows Tables sur un GPU ?

Rainbow Table probabilistes

- Sur GPU beaucoup de nouvelles contraintes se posent. L'algorithme doit être modifié en conséquence :
 - Divergence de Threads dans un WARP
 - Diverses mémoires de caractéristiques différentes
 - Parallélisations massive
 - Synchronisation des threads
 - Communication RAM \Leftrightarrow CG
 - ...

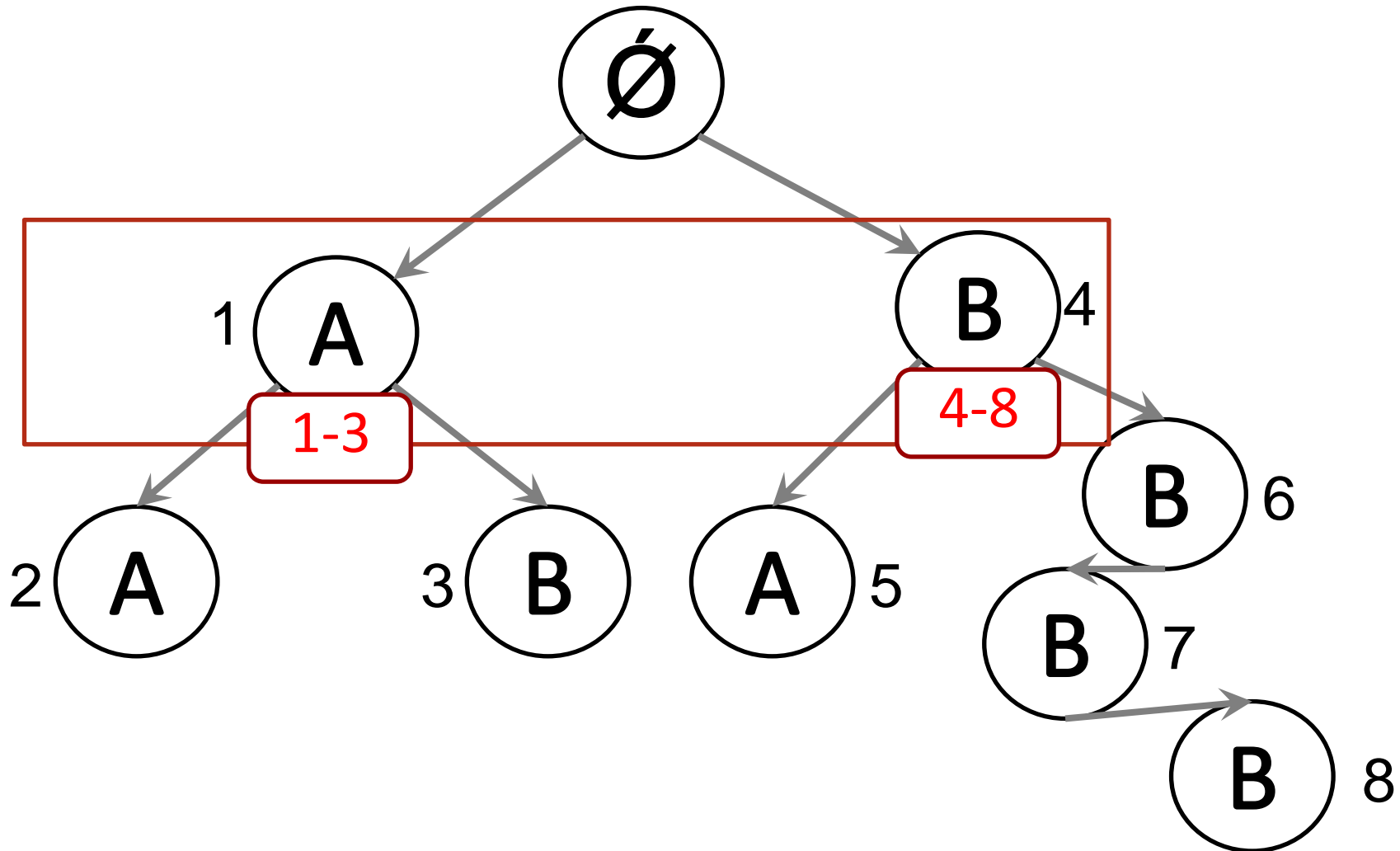
Rainbow Table probabilistes

- Exemple : recherche itérative → recherche dichotomique



Rainbow Table probabilistes

- Exemple : recherche itérative → recherche dichotomique



Sommaire

Introduction

Complexité d'un mot de passe

Rainbow Tables

Rainbow Tables probabilistes

► **Éléments de performance**

Contre-mesures

Questions ?

Éléments de performance

- Présentation des métriques :
 - ROCKYOU : Site web populaire qui stockait les mots de passe en clair : 32 603 388 mots de passe.
 - 500K : Ensemble de caractéristiques de 500 000 mots de passe obtenus en tests d'intrusion réels au cours des quelques mois passés.

Éléments de performance

- Dans le cadre d'une utilisation nomade :
 - 30 millions de hashes calculés à la seconde :

Espace parcouru	Temps requis	Rockyou	500K
LowerAlphaNum 1-7	1h	46%	9%
LowerAlphaNum 1-8	26h	64%	49%
MixedAlphaNum 1-7	32h	48%	13%
LowerAlpha 1-9	50h	35%	6%

Éléments de performance

- Dans le cadre d'une utilisation nomade :
 - Quelques GO (disque dur d'ordinateur portable) :

Espace parcouru	Taille de la rainbow	Rockyou	500K
LowerAlphaNum 1-7	0,3G	46%	9%
LowerAlphaNum 1-8	12G	64%	49%
MixedAlphaNum 1-7	15G	48%	13%
LowerAlpha 1-9	23G	35%	6%

Éléments de performance

- Dans le cadre d'une utilisation nomade :
 - Quelques Go (disque dur d'ordinateur portable) :

Espace parcouru	Taille de la rainbow	Rockyou	500K
Markov 265 optim	1,04Go (4x267M)	71%	58%
Markov 265	1,11Go(4x283M)	75%	50%
Markov 285 optim	7,99Go (4x2,00G)	79%	69%
Markov 285	8,50Go (4x2,13G)	83%	60%
Markov 300 optim	36,76Go (4x9,19Go)	84%	76%
Markov 300	39,19Go (4x9,80Go)	87%	66%

Éléments de performance

- Dans le cadre d'une plateforme spécialisée :
 - (Très) gros disques dur :

Espace parcouru	Taille de la rainbow	Rockyou	500K
MixedAlphaNum 1-8	900 Go	68%	63%
LowerAlphaNum 1-10	15 000 Go	83%	55%
LowerAlpha 1-11	15 000 Go	39%	7%
AllChars 1-8	?	69%	68%

Éléments de performance

- Dans le cadre d'une plateforme spécialisée :
 - (Très) gros disques dur :

Espace parcouru	Taille de la rainbow	Rockyou	500K
Markov 315 optim	270Go (4x67Go)	87%	81%
Markov 315	286Go (4x71Go)	89%	71%
Markov 335 optim	2 To (4x512Go)	91%	86%
Markov 335	2,15To (4x550Go)	92%	78%

Sommaire

Introduction

Complexité d'un mot de passe

Rainbow Tables

Rainbow Tables probabilistes

Éléments de performance

▶ **Contre-mesures**

Questions ?

Contre-mesures

- Contre les Rainbow Tables:
 - Salez, salez, salez
- Contre Markov:
 - Utilisez des mots longs
 - Utilisez des caractères nationaux/exotiques
 - Auditez vos mots de passe
 - Générez vos mots de passe aléatoirement

Conclusion

- <http://www.lexsi.com/francais/cracknfast>

INNOVATIVE SECURITY

Pour vous aider à maîtriser
vos risques

SIEGE SOCIAL :
Tours Mercuriales Ponant
40 rue Jean Jaurès
93170 Bagnolet
Tél. (+33) 01 55 86 88 88

www.lexsi.com

LEXSI LYON

Bois des Côtes 1 - Bâtiment A
300 Route Nationale 6
69760 LIMONEST
Tél. (+33) 08 20 02 55 20

LEXSI CANADA

1010, rue de la Gauchetière Ouest
Bureau M110
Montréal QC H3B 2N2
Tél. +1 514 903 6560

LEXSI SINGAPORE

60 Bayshore Road / Bayshore Park
#10-07 - Jade Tower
469982 - Singapore
Tél. +65 65191705