



Les fonctions de hachage



Rachelle Heim Boissier

Finale du concours Alkindi



Une fonction de hachage, c'est quoi ?

Une fonction de hachage, c'est quoi ?

Objectif : condenser une information longue

Une fonction de hachage, c'est quoi ?

Objectif : condenser une information longue



Message



Fonction de hachage



Empreinte

Une fonction de hachage, c'est quoi ?

Objectif : condenser une information longue



Premier exemple

Pouvez-vous proposer une fonction de hachage qui, en 2 caractères, condense l'information "identité d'une personne" ?



Premier exemple

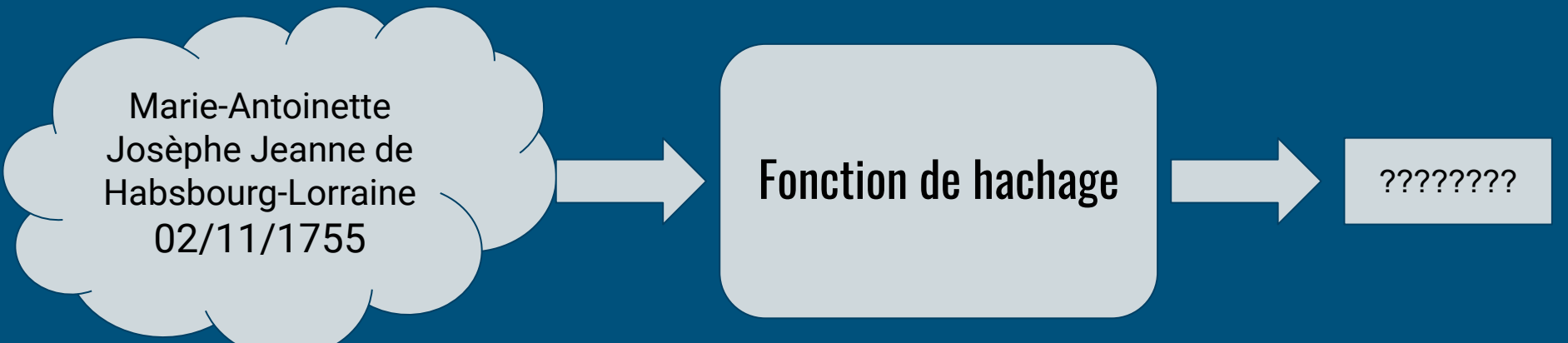
Pouvez-vous proposer une fonction de hachage qui, en 2 caractères, condense l'information "identité d'une personne" ?

Proposition : les initiales



Premier exemple

Pouvez-vous proposer une fonction de hachage qui, en 8 caractères, condense l'information "identité d'une personne" ?



```
graph LR; A([Marie-Antoinette  
Josèphe Jeanne de  
Habsbourg-Lorraine  
02/11/1755]) --> B[Fonction de hachage]; B --> C[????????];
```

Marie-Antoinette
Josèphe Jeanne de
Habsbourg-Lorraine
02/11/1755

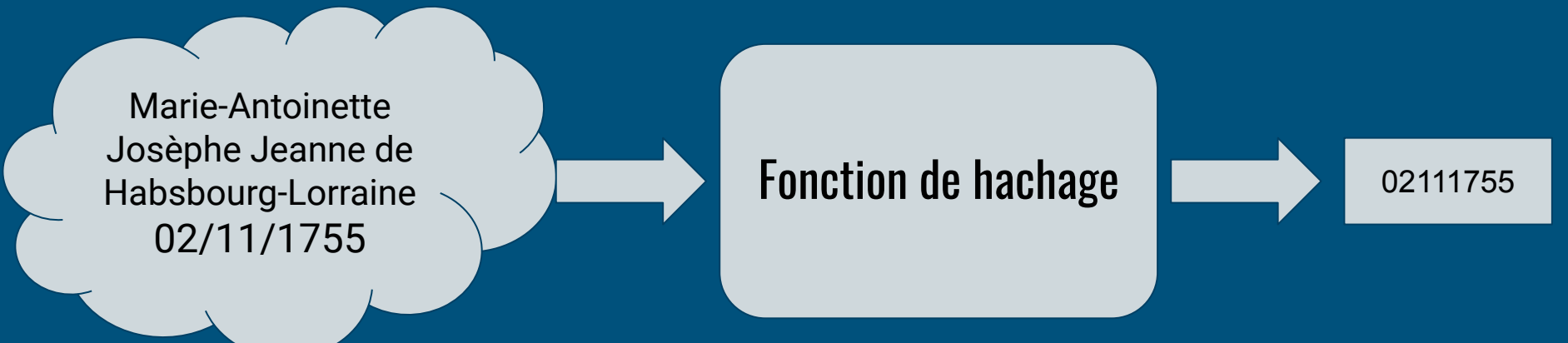
Fonction de hachage

????????

Premier exemple

Pouvez-vous proposer une fonction de hachage qui, en 8 caractères, condense l'information "identité d'une personne" ?

Proposition : la date de naissance



```
graph LR; A([Marie-Antoinette  
Josèphe Jeanne de  
Habsbourg-Lorraine  
02/11/1755]) --> B[Fonction de hachage]; B --> C[02111755]
```

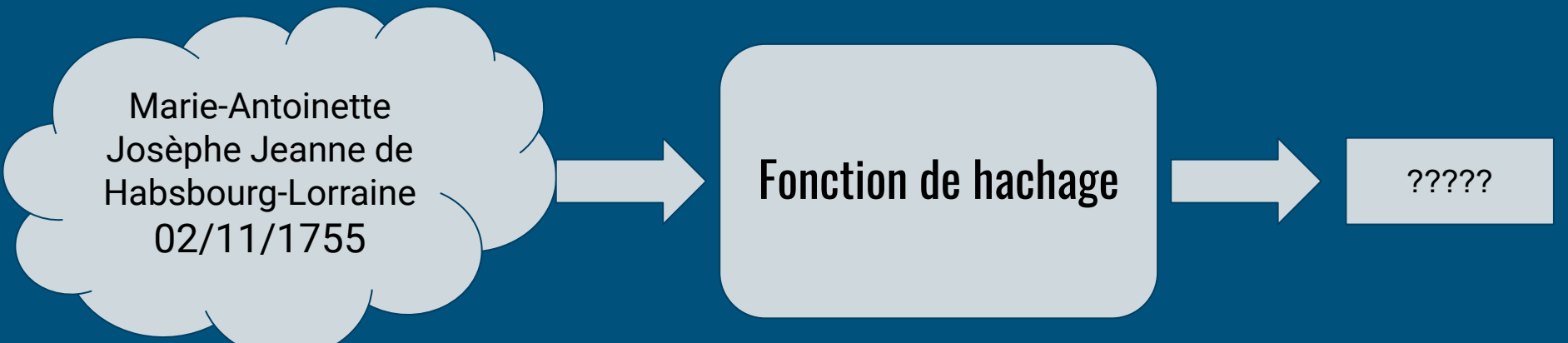
Marie-Antoinette
Josèphe Jeanne de
Habsbourg-Lorraine
02/11/1755

Fonction de hachage

02111755

Premier exemple

Pouvez-vous proposer une fonction de hachage qui, en 5 caractères, condense l'information "identité d'une personne" ?



```
graph LR; A([Marie-Antoinette  
Josèphe Jeanne de  
Habsbourg-Lorraine  
02/11/1755]) --> B[Fonction de hachage]; B --> C[?????]
```

Marie-Antoinette
Josèphe Jeanne de
Habsbourg-Lorraine
02/11/1755

Fonction de hachage

?????

Premier exemple

Pouvez-vous proposer une fonction de hachage qui, en 4 caractères, condense l'information "identité d'une personne" ?

Proposition : première lettre du prénom "doublée" + sommer les chiffres associés aux initiales, ajouter à l'année de naissance, garder les 4 derniers chiffres obtenus

Marie-Antoinette
Josèphe Jeanne de
Habsbourg-Lorraine
02/11/1755

Fonction de hachage

Y1792

Les fonctions de hachage cryptographiques

3 propriétés de sécurité :

Les fonctions de hachage cryptographiques

3 propriétés de sécurité :

- I. Il doit être difficile de trouver deux messages différents qui ont la même empreinte

Les fonctions de hachage cryptographiques

3 propriétés de sécurité :

- I. Il doit être difficile de trouver deux messages différents qui ont la même empreinte
- II. Si on me donne une empreinte aléatoire, il doit être difficile de trouver un message qui donne cette empreinte

Les fonctions de hachage cryptographiques

3 propriétés de sécurité :

- I. Il doit être difficile de trouver deux messages différents qui ont la même empreinte
- II. Si on me donne une empreinte aléatoire, il doit être difficile de trouver un message qui donne cette empreinte
- III. Si on me donne un message aléatoire et son empreinte, il doit être difficile de trouver un autre message qui a la même empreinte

Les fonctions de hachage cryptographiques

3 propriétés de sécurité :


- I. Il doit être difficile de trouver deux messages différents qui ont la même empreinte
- II. Si on me donne une empreinte aléatoire, il doit être difficile de trouver un message qui donne cette empreinte
- III. Si on me donne un message aléatoire et son empreinte, il doit être difficile de trouver un autre message qui a la même empreinte

→ **Et dans le cas des anniversaires, ça donne quoi?**

Les fonctions de hachage cryptographiques

3 propriétés de sécurité :

- I. Il doit être difficile de trouver deux messages différents qui ont la même empreinte
- II. Si on me donne une empreinte aléatoire, il doit être difficile de trouver un message qui donne cette empreinte
- III. Si on me donne un message aléatoire et son empreinte, il doit être difficile de trouver un autre message qui a la même empreinte



Notre travail
aujourd'hui

Les fonctions de hachage cryptographiques

3 propriétés de sécurité :

- I. Il doit être difficile de trouver deux messages différents qui ont la même empreinte
- II. Si on me donne une empreinte aléatoire, il doit être difficile de trouver un message qui donne cette empreinte
- III. Si on me donne un message aléatoire, il doit être difficile de trouver un autre message qui donne la même empreinte

Deux messages différents
qui ont la même empreinte
sont appelés "**collision**"

(Crypt)analyser des fonctions de hachage

Objectifs :

- 1) Déterminer si des fonctions de hachage sont sûres contre la recherche de collision
- 2) Proposer des fonctions de hachage

Première proposition



Message	Empreinte
12	02

Ma fonction de hachage prend en entrée des messages de longueur paire. Les empreintes ont deux chiffres.

Première proposition



Message	Empreinte
12	02
68	48

Ma fonction de hachage prend en entrée des messages de longueur paire. Les empreintes ont deux chiffres.

Première proposition



Message	Empreinte
12	02
68	48
1110	10

Ma fonction de hachage prend en entrée des messages de longueur paire. Les empreintes ont deux chiffres.

Première proposition



Message	Empreinte
12	02
68	48
1110	10
1211	32

À vous de jouer! Pouvez-vous trouver une collision?

Comment fonctionne ma fonction ?

- $12 \rightarrow 1|2 \rightarrow 1 \times 2 = 2 \rightarrow 02$
- $68 \rightarrow 6|8 \rightarrow 6 \times 8 = 48 \rightarrow 48$
- $1110 \rightarrow 11|10 \rightarrow 11 \times 10 = 110 \rightarrow 10$
- $1211 \rightarrow 12|11 \rightarrow 12 \times 11 = 132 \rightarrow 32$

Message	Empreinte
12	02
68	48
1110	10
1211	32

Comment fonctionne ma fonction ?

- $12 \rightarrow 1|2 \rightarrow 1 \times 2 = 2 \rightarrow 02$
- $68 \rightarrow 6|8 \rightarrow 6 \times 8 = 48 \rightarrow 48$
- $1110 \rightarrow 11|10 \rightarrow 11 \times 10 = 110 \rightarrow 10$
- $1211 \rightarrow 12|11 \rightarrow 12 \times 11 = 132 \rightarrow 32$

Message	Empreinte
12	02
68	48
1110	10
1211	32

À vous de jouer! Pouvez-vous trouver une collision?

Plusieurs possibilités

- **Les messages miroirs**

Exemple : 68 et 86 donnent la même empreinte

Plusieurs possibilités

- **Les messages miroirs**

Exemple : 68 et 86 donnent la même empreinte

- **Les nombres dont une moitié des chiffres sont égaux à 0**

Exemple : 10 et 1100 donnent 0

Deuxième proposition



Message	Empreinte
12	08
68	
1110	
1111	

Deuxième proposition



Message	Empreinte
12	08
68	70
1110	
1111	

Deuxième proposition



Message	Empreinte
12	08
68	70
1110	44
1111	

Deuxième proposition



Message	Empreinte
12	08
68	70
1110	44
1111	56

À vous de jouer! Pouvez-vous trouver une collision?

Comment fonctionne ma fonction ?

- 12 → 1|2 → $(1+1) \times (2+2) = 8$ → 08
- 68 → 6|8 → $(6+1) \times (8+2) = 70$ → 70
- 1110 → 11|10 → $(11+1) \times (10+2) = 144$ → 44
- 1111 → 11|11 → $(11+1) \times (11+2) = 156$ → 56

Message	Empreinte
12	08
68	70
1110	44
1111	56

Comment fonctionne ma fonction ?

- 12 \rightarrow 1|2 \rightarrow $(1+1) \times (2+2) = 8 \rightarrow 08$
- 68 \rightarrow 6|8 \rightarrow $(6+1) \times (8+2) = 70 \rightarrow 70$
- 1110 \rightarrow 11|10 \rightarrow $(11+1) \times (10+2) = 144 \rightarrow 44$
- 1111 \rightarrow 11|11 \rightarrow $(11+1) \times (11+2) = 156 \rightarrow 56$

Message	Empreinte
12	08
68	70
1110	44
1111	56

À vous de jouer! Pouvez-vous trouver une collision?

Trouver une collision

- **Remarques :**

→ Les messages symétriques ne donnent plus la même empreinte :
68 donne 70, 86 donne 72

→ On ne peut plus obtenir l'empreinte 00 en ne mettant que des 0 d'un côté

- **Proposition :**

68 → 6|8 → $(6+1) \times (8+2) = 7 \times 10 = 70$ → 70

On veut obtenir 10x7

On prend donc (10-1) et (7-2).

95 et 68 donnent la même empreinte

À vous de jouer!

Travail en groupe de 5 personnes

Pouvez-vous concevoir une fonction de hachage résistante à la recherche de collisions dont les messages font 3 chiffres?

... vos camarades essaieront ensuite de l'attaquer!