

ISIFC 3, Crypto Fonctions de hachage

Jean-François COUCHOT
Université de Franche-Comté, UFR-ST

Plan

Introduction

Théorie

Constructions



Introduction

Applic° crypto. : l'intégrité

Applic° crypto. : hachage de mots de passe

Applic° crypto. : code d'Authentification de Message

Applic° non crypto. : pseudonymisation

Théorie

Constructions



Plan



Introduction

Applic° crypto. : l'intégrité

Applic° crypto. : hachage de mots de passe

Applic° crypto. : code d'Authentification de Message

Applic° non crypto. : pseudonymisation

Théorie

Constructions



Objectif d'intégrité : vérifier l'égalité $m_1 = m_2$

Pour ne pas analyser tous les bits de m_1 et m_2 (fastidieux)

- Souhait : une fonction H
 - Réduisant m à son empreinte $H(m)$ de taille fixe
 - Implémentant l'effet d'avalanche : même si m_1 et m_2 ne diffèrent que d'1 bit $\rightsquigarrow H(m_1)$ et $H(m_2)$ complètement différents
 - Reproductible : $H(m)$ ne change pas au cours du temps

Exécution de la fonction sha256 sur 2 messages proches

```
import hashlib
txt1 = " ISIFC Crypto".encode('utf-8')
print(txt1, '\n', hashlib.sha256(txt1).hexdigest())
txt2 = " ISIFB Crypto".encode('utf-8')
print(txt2, '\n', hashlib.sha256(txt2).hexdigest())

b' ISIFC Crypto'
f5fea6cc095c19cb722f1731560bb8765971810b64b863331169220863be27a1
b' ISIFB Crypto'
8aac87441cbf30978adf41f8347b5cb3a35e876d1551dfc79d2851ba5396373d
```

Plan



Introduction

Applic° crypto. : l'intégrité

Applic° crypto. : hachage de mots de passe

Applic° crypto. : code d'Authentification de Message

Applic° non crypto. : pseudonymisation

Théorie

Constructions



Mot de passe : jamais stocké en clair !

Hachage de mots de passe

Le hachage de mots de passe est un cas particulier très usuel d'utilisation des fonctions de hachage. L'idée principale :

1. Utilisateur ou utilisatrice : définit son mot de passe m ;
2. Système : enregistre une empreinte $h = H(m)$ du mot de passe ;
3. Lors d'une connexion : mot de passe m' saisi ;
4. Système : calcule l'empreinte $h' = H(m')$ du mot de passe puis, comparaison avec h .

Stockage de mot de passe dans une base

```
CREATE TABLE ETUDIANT
(Numero INTEGER PRIMARY KEY,
Nom VARCHAR(50) NOT NULL,
Prenom VARCHAR(50) NOT NULL,
DateNaissance DATE NOT NULL,
Login CHAR(8) NOT NULL UNIQUE,
MotDePasse BINARY(64) NOT NULL)
```

```
INSERT INTO ETUDIANT
VALUES (32823, 'Marche', 'Claire',
'1998-10-01', 'cmarche',
SHA2('@tbNU67z',512)) -- pertinence cette
```

Hachage de mots de passe : attaques



- ▶ l'espace de recherche est-il suffisamment grand ?
- ▶ la fonction de hachage utilisée est-elle rapide ?



Espace de recherche

Espace de recherche

Ce paramètre dépend de l'utilisateur. Si l'utilisateur utilise un mot du dictionnaire, l'espace de recherche est ridiculement faible !

- ▶ mots du dictionnaire : $130000 \approx 2^{17}$
- ▶ deux mots du dictionnaire : 2^{34}
- ▶ trois mots du dictionnaire : 2^{51}

Ordres de grandeur

Règles en vigueur sur l'ENT : a minima

- ▶ 8 caractères
- ▶ 1 caractère alphabétique (parmi 26)
- ▶ 2 chiffres
- ▶ 1 caractère spécial

Longueur	6	7	8	9	10
a-z (26)	2^{28}	2^{32}	2^{37}	2^{42}	2^{47}
a-zA-Z (52)	2^{34}	2^{39}	2^{45}	2^{51}	2^{57}
a-zA-Z0-9 (62)	2^{35}	2^{41}	2^{47}	2^{53}	2^{59}
+ [punct] (94)	2^{39}	2^{45}	2^{52}	2^{58}	2^{65}
ENT	-	-	2^{48}	2^{55}	2^{61}

Vitesse de la fonction de hachage

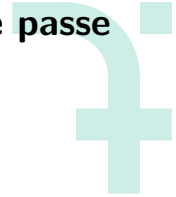


Vitesse de la fonction de hachage

- ▶ Une fonction de hachage est normalement destinée à être rapide pour être capable de hacher de grandes quantités de données.
- ▶ Pour limiter la portée d'une attaque sur des mots de passe, on a intérêt à ce que la fonction de hachage soit la plus lente possible.
- On n'utilise pas les mêmes fonctions de hachages pour les mots de passe et pour les autres utilisations cryptographiques



Hachage cryptographique pour les mots de passe



Généralités

Dans les fonctions suivantes, on peut souvent régler :

- ▶ le temps d'exécution
- ▶ l'espace mémoire utilisé

Hachage cryptographique de mots de passe

- ▶ bcrypt, 1999, basé sur Blowfish
- ▶ PBKDF2, 2000
- ▶ scrypt, 2012
- ▶ Argon2, 2015, gagnant du Password Hashing Competition





Introduction

Applic° crypto. : l'intégrité

Applic° crypto. : hachage de mots de passe

Applic° crypto. : code d'Authentification de Message

Applic° non crypto. : pseudonymisation

Théorie

Constructions



Code d'Authentification de Message



Définition (Code d'Authentification de Message (MAC))

Un **Message Authentication Code** (MAC) est une association entre une fonction de compression et une clef secrète permettant de vérifier à la fois l'intégrité et l'authenticité des données reçues.

Utilisation

1. Alice veut envoyer un message m à Bob
2. Elle calcule le MAC avec une clef secrète K qu'elle partage avec Bob
3. Elle envoie son message et le MAC à Bob
4. Bob recalcule le MAC et vérifie qu'il est identique à celui d'Alice



Hash-based Message Authentication Code (HMAC)

Hash-based Message Authentication Code (HMAC)

- ▶ Utilisé dans IPSec et TLS
- ▶ $\text{HMAC}(K, m) = H((K \oplus \text{opad}) \parallel H((K \oplus \text{ipad}) \parallel m))$
 - ▶ H est une fonction de hachage cryptographique
 - ▶ K est la clef secrète
 - ▶ $\text{opad} = 0x5c5c5c \dots 5c5c$
 - ▶ $\text{ipad} = 0x363636 \dots 3636$
 - ▶ $\parallel$ est la concaténation
- ▶ Plusieurs variantes suivant H : HMAC-MD5 (possible, mais cata!), HMAC-SHA-256





Introduction

Applic° crypto. : l'intégrité

Applic° crypto. : hachage de mots de passe

Applic° crypto. : code d'Authentification de Message

Applic° non crypto. : pseudonymisation

Théorie

Constructions



Pseudonymiser un attribut identifiant

Pseudonymiser n'est pas anonymiser

- ▶ Remplacer la valeur d'un attribut "identifiant" par un pseudonyme.
- ▶ Pseudonyme peut être dérivé de la valeur identifiante (par exemple, en appliquant une fonction de hachage).
- ▶ Risque de mise en corrélation de données avec l'identité originale d'un sujet : réduit mais possible
- ▶ **ré-identification** indirecte possible en utilisant les autres attributs → **Pas une méthode d'anonymisation.**

Pseudonymiser un attribut avec pandas

```
import pandas as pd
import hashlib

df = pd.read_csv('BankChurners.csv',
                 usecols=['CLIENTNUM', 'Customer_Age', 'Total_Trans_Amt'])
df['CLIENTNUM'] = df['CLIENTNUM'].astype(str)
df['CLIENTNUM_HASH'] = df['CLIENTNUM'].apply(lambda x:
                                              hashlib.sha256(x.encode('utf-8'))
                                              .hexdigest())

df.drop(['CLIENTNUM'], inplace=True)
```



Plan

Introduction

Théorie

Formalisation

Recherche de collisions

Constructions



Plan

Introduction

Théorie

Formalisation

Recherche de collisions

Constructions





Définition (Fonction de hachage $H : \mathbb{B}^* \rightarrow \mathbb{B}^n$)

Fonction qui transforme un message m de taille quelconque en une valeur $h = H(m)$ de taille fixe n .

- ▶ h : appelé.e empreinte, le résumé ou la somme de contrôle de m
- ▶ m : appelé.e l'antécédent ou la préimage de h

Définition (Collision)

Il y a collision entre m_1 et m_2 , $m_1 \neq m_2$ si $H(m_1) = H(m_2)$



Propriétés pour $H : \mathbb{B}^* \rightarrow \mathbb{B}^n$

Définition (Résistance à la préimage)

Pour toute empreinte h , il est difficile de trouver m tel que $H(m) = h$.

Conséquences :

- ▶ Difficile de retrouver un mdp m étant donnée une empreinte h stockée
- ▶ On parle de fonction à sens unique

Définition (Résistance à la seconde préimage)

Pour tout m_1 , il est difficile de trouver $m_2 \neq m_1$ tel que $H(m_1) = H(m_2)$.

Remarque : on a ici une connaissance supplémentaire qui est m_1

Définition (Résistance aux collisions)

Il est difficile de trouver m_1 et $m_2 \neq m_1$ tels que $H(m_1) = H(m_2)$.

Remarque : comme $H : \mathbb{B}^* \rightarrow \mathbb{B}^n$, il y a nécessairement des collisions



Plan



Introduction

Théorie

Formalisation

Recherche de collisions

Constructions



#tirages avant une collision avec une proba. p ?

Proba. d'une coll. en tirant au hasard k éléments parmi n distincts ?

- 1^{er} tirage : il y a n valeurs différentes parmi lesquelles choisir.
2. Proba. que les deux 1^{ers} tirages soient $\neq$: $\frac{n-1}{n}$.
3. Proba. que les trois 1^{ers} tirages soient $\neq$: $\frac{n-1}{n} \times \frac{n-2}{n}$
4. ... Proba. que les k 1^{ers} tirages soient $\neq$: $\frac{n-1}{n} \times \frac{n-2}{n} \times \dots \times \frac{n-(k-1)}{n}$.

⇒ Proba. p d'obtenir au moins une coll. sur k tirages :

$$p = 1 - \frac{n!}{(n-k)!} \cdot \frac{1}{n^k} \approx 1 - e^{-\frac{k(k-1)}{2n}} \text{ croissante en en fct. de } k$$

⇒ Nbre. k de tirages suffisants pour avoir une coll. avec une proba. p :

$$k \approx \sqrt{2 \cdot n \ln \left(\frac{1}{1-p} \right)}$$

Applications

- ▶ Paradoxe des anniversaires : nbre. suffisant de personnes pour que la proba. qu'au moins deux aient leur anniversaire le même jour soit sup. à $\frac{1}{2}$? 23.
- ▶ Conséquences pour H sur N bits : collision avec une probabilité supérieure à $\frac{1}{2}$ en $O(\sqrt{2^N}) = O(2^{\frac{N}{2}})$: seulement $\frac{N}{2}$ bits de sécurité.

Plan



Introduction

Théorie

Constructions

Fonctions de hachage issues de Merkle-Damgård
SHA-3



Plan



Introduction

Théorie

Constructions

Fonctions de hachage issues de Merkle-Damgård

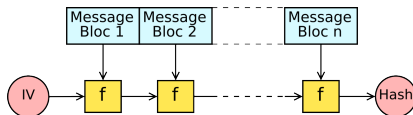
SHA-3



Construction de Merkle-Damgård

Idées principales

- ▶ On découpe le message m en blocs m_i de taille égale
- ▶ On utilise une fonction de compression $f : h_0 = IV, h_{i+1} = f(m_i, h_i)$
- ▶ Propriété : si f est résistante aux collisions, alors la construction l'est
- ▶ Appliquées dans MD5, SHA-1, SHA-2.....

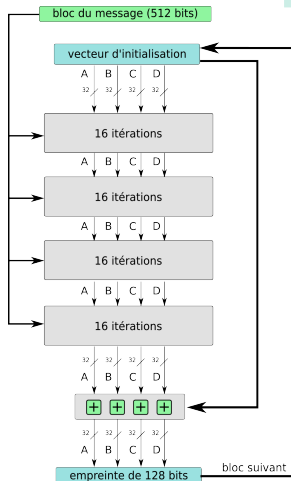


MD5

Aperçu général

Généralités

- ▶ Inventé par Ronald Rivest en 1991
- ▶ Amélioration de MD4
- ▶ Bloc de 512 bits
- ▶ Empreinte de 128 bits
- ▶ 64 rondes (ou itérations)



MD5

pas résistance à la préimage



Historique

- ▶ 2009 : Attaque en $2^{123.4}$

Attaque hashcat de example0.hash stockant des empreintes MD5 (-m 0)

- ▶ `hashcat -m 0 -a 0 example0.hash example.dict -r dive.rule`

Avec un dictionnaire (`-a 0 example.dict`) et des règles (`-r dive.rule`)
↪ 1695 mdp reconstruits en qqes. minutes

- ▶ `hashcat -m 0 -a 3 example0.hash`

Brute force (`-a 3`) ↪ 1900 mdp reconstruits en une heure



MD5

pas résistante aux collisions

Historique $\rightsquigarrow$ MD5 n'est plus une fonction cryptographiquement sûre

- ▶ 1996 : une faille est trouvée dans la fonction de compression
- ▶ 2004 : premières collisions générées

Code de collision

```
import hashlib
from array import array

input1 = array('I', [1634021390, 2275908181, 4156951504, 889109771, 1694748420, 2236575902,
                     4212113460, 2269944933, 798280768, 362884587, 1544942755, 1225230011,
                     1835370099, 2754879357, 2413254944, 4023487834])

input2 = array('I', [1634021390, 2275908181, 4156951504, 889109771, 1694748420, 2236576926,
                     4212113460, 2269944933, 798280768, 362884587, 3692426403, 1225230011,
                     1835370099, 2754879357, 2413254944, 4023487834])

print(">"+str(input1[5])+" vs "+ str(input2[5]))
print(">"+str(input1[10])+" vs "+ str(input2[10]))

print(hashlib.md5(input1).hexdigest())
print(hashlib.md5(input2).hexdigest())

2236575902 vs 2236576926
1544942755 vs 3692426403
cee9a457e790cf20d4bdaa6d69f01e41
cee9a457e790cf20d4bdaa6d69f01e41
```

SHA-1

Aperçu général et attaques

Algorithme similaire à MD-5, mais

- ▶ 1995 : complexification de SHA-0
- ▶ Empreinte de 160 bits
- ▶ 80 rondes (ou itérations)

Attaques

- ▶ 2005 : construction d'une attaque théorique en 2^{69} (comparer à 2^{80})
- ▶ 2017 : attaque de la seconde préimage réaliste (Google)
- ▶ 2020 : construction d'une attaque théorique 2^{63} opérations.
- ▶ Déconseillées depuis 2010, mais :
 - ▶ Signatures SHA-1 (vues plus tard) : encore acceptées dans TLS...
 - ▶ HMAC-SHA-1 : dans plus de 8% des 1M de serveurs Alexa (2020)
- ▶ Il est important que **vous ne l'utilisiez plus !**

SHA-256

Aperçu général



Algorithme similaire à SHA-1, mais

- ▶ 2002 : création par la National Security Agency
- ▶ Empreinte de 256 bits
- ▶ 64 rondes (ou itérations)

Attaques

- ▶ Aucune connue ! A utiliser (et sa version SHA-512)



Plan



Introduction

Théorie

Constructions

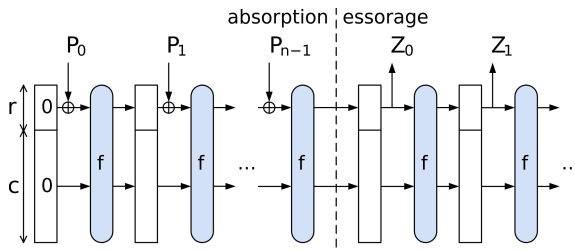
Fonctions de hachage issues de Merkle-Damgård

SHA-3



SHA-3 Keccak : construction éponge

En image¹



Algorithme

Absorption :

- ▶ état interne S : initialisé à zéro
- ▶ pour chaque bloc B de r bits de $P(\text{chaîne})$:
- ▶ R : remplacé par $R \oplus B$
- ▶ S : remplacé par $f(S)$

Pour l'essorage, répéter :

- ▶ sortir la portion R de S
- ▶ S est remplacé par $f(S)$

1. https://en.wikipedia.org/wiki/Sponge_function