Licence Informatique

Introduction à la Cryptographie

Exercices de TD et TP

Gilles Dequen

1 Ordre de grandeur

On souhaite vider les océans avec un dé à coudre. On considère qu'un dé à coudre est un cylindre de 1.5 cm de hauteur pour 1.5 cm de diamètre. Selon l'Institut Français des Mers, les océans couvrent 360 millions de km^2 avec une profondeur moyenne de 3800m. Estimez le nombre de dés à coudre que contiennent les océans. Déduisez-en un encadrement entre deux puissances de 2 [1].

2 Paradoxe des anniversaires

2.1 Introduction

Supposons que des codes confidentiels de 4 chiffres sont distribués au hasard. Combien de personnes doit-on rassembler pour que la probabilité que deux personnes aient le même code soit de $\frac{1}{2}$?

2.2 Collisionnement d'une fonction de hachage

Sur la base du principe de calcul du paradoxe des anniversaires, estimez le nombre d'itérations moyennes nécessaires au collisionnement de la fonction de hachage `SHA-256` avec une probabilité de 0.8. Vous pouvez le faire par le biais d'une simulation numérique - une dichotomie par exemple - ou directement par le calcul. Pour mémoire, l'empreinte `SHA-256` a une taille d'exactement 256 bits.

2.2.1 ... et sur une preuve de travail

On considère maintenant un cas d'école. Quelle serait le nombre d'itérations nécessaires au collisionnement des k premiers bits d'une fonction de hachage H avec une probabilité de p ?

2.3 Estimation d'une attaque par paradoxe

Le facteur de travail d'un algorithme est le nombre d'instructions élémentaires nécessaires à son exécution. La puissance d'une machine est le nombre

1. Le volume d'un cyclindre de rayon r et de hauteur h est égal à $\pi \times r^2 \times h$

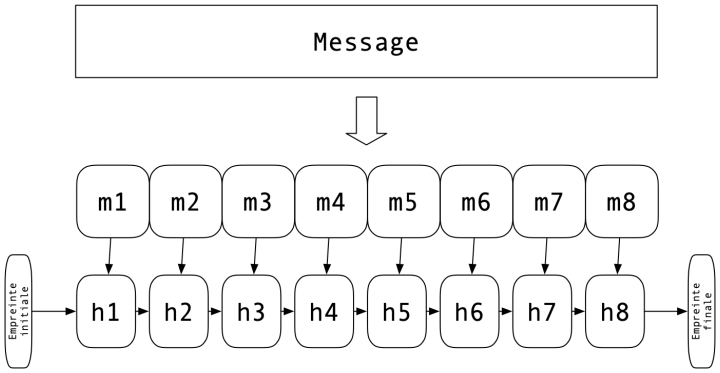
d'instructions qu'elle exécute par unité de temps. La plus grande puissance brute pouvant actuellement être développée par un CPU en « single socket » est celle du AMD RYZEN 9 7950X [2]. Poussé dans ses retranchements par l'overclocking, il atteint 293038 MIPS [3] sur le benchmark « `7-Zip` ». On considérera que c'est notre PC de référence pour cet exercice. Le facteur de travail d'une implémentation de SHA-256 pour hacher un message sur un bloc (512 bits) est d'environ 900 instructions élémentaires.

- Estimez le temps nécessaire pour collisionner SHA-256 pour notre PC de référence.
- Estimez le temps nécessaire pour collisionner SHA-256 si l'on dispose de l'ensemble des 3.10^9 ordinateurs disponibles sur Terre. On considère pour plus de simplicité que un *ordinateur* est équivalent à un *PC de référence*.

3 Fonction de Hachage : adaptation de Toy Tetragraph Hash (TTH)

On considère une fonction de hachage inspirée de TTH que l'on nommera TTH_{64}^5 qui travaille sur des valeurs numériques modulo 64 (i.e $[0, ..., 63]$) et dont l'empreinte résultante est constituée de 5 valeurs. Par ailleurs, TTH_{64}^5 travaille sur une partition en blocs de 25 valeurs. TTH_{64}^5 considère un message clair M sous forme binaire. Dans l'hypothèse où la taille de M n'est pas multiple de 25, le bloc incomplet résultant de cette situation est complété par la valeur 32 puis autant de valeurs 0 que nécessaire pour le compléter. On parle dans ce cas de *padding* ou de *bourrage* de M.

Le schéma ci-dessous vous donne le schéma général d'un chiffrement (ici un hachage) par blocs.



On considèrera à titre d'exemple que M est l'expression d'un message clair ré-encodé sur des valeurs entières non signées comprises entre 0 et 63. On pose :

2. `https://hwbot.org/hardware/processor/ryzen_9_7950x`
3. Millions d'Instructions Par Secondes

$$M = \{00, 06, 08, 35, 17, 28, 24, 56, 62, 07, 12, 16, 20, 05, 33, 43, 35, 27, 12, 60, \\ 25, 23, 18, 01, 45, 56, 12, 34, 21, 20, 02, 10, 22, 20, 17, 34, 01\} \quad (1)$$

On considère également que l'empreinte est initialement un vecteur nul d'ordre 5, soit :

00	00	00	00	00

Empreinte

Les différentes étapes de $TTH_{64}^{5}(M)$ sont les suivantes :

A) Padding de M

Aprés la phase de *padding*, on a :

$$M_{+padding} = \{00, 06, 08, 35, 17, 28, 24, 56, 62, 07, 12, 16, 20, \\ 05, 33, 43, 35, 27, 12, 60, 25, 23, 18, 01, 45, 56, 12, 34, 21, \\ 20, 02, 10, 22, 20, 17, 34, 01, 32, 00, 00, 00, 00, 00, 00, 00, \\ 00, 00, 00, 00, 00, \} \quad (2)$$

B) Arrangement matriciel de $M_{+padding}$

$M_{+padding}$ est divisé en blocs successifs de 25 valeurs qui sont réparties dans des matrices 5×5 en suivant le sens de lecture de la gauche vers la droite et ligne par ligne. A partir de notre exemple, on obtient les matrices suivantes :

00	06	08	35	17
28	24	56	62	07
12	16	20	05	33
43	35	27	12	60
25	23	18	01	45

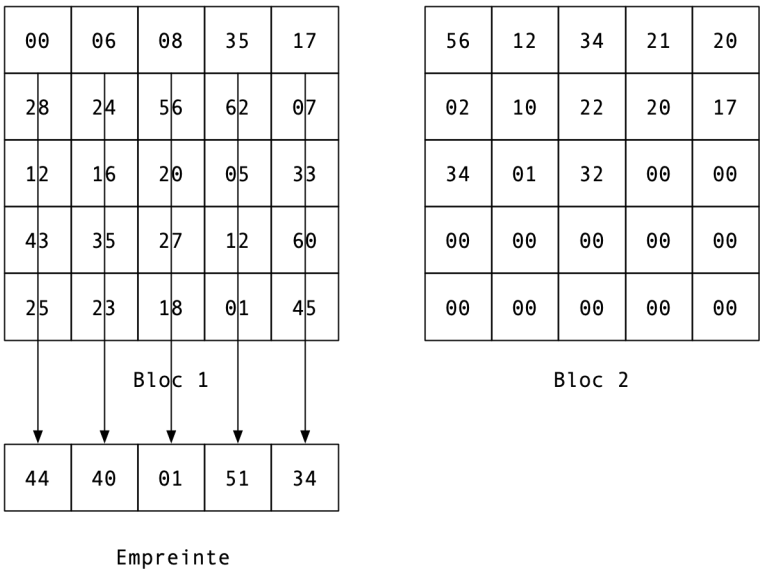
Bloc 1

56	12	34	21	20
02	10	22	20	17
34	01	32	00	00
00	00	00	00	00
00	00	00	00	00

Bloc 2

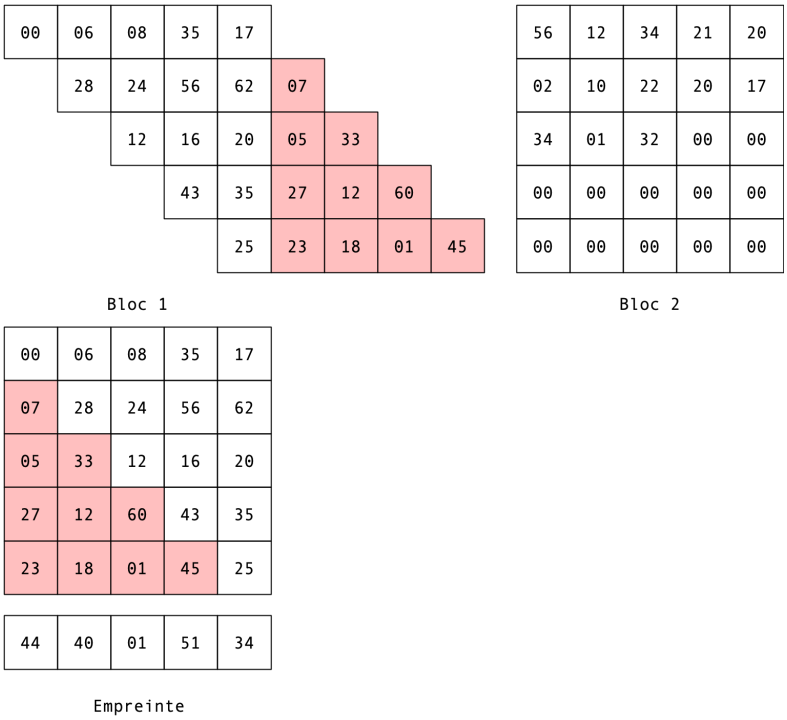
C) Calcul de l'empreinte pour le bloc en cours - étape 1

A l'empreinte courante est ajoutée la somme de chaque colonne en regard du bloc en cours. Ce cumul se fait modulo 64. Pour notre exemple, on a :



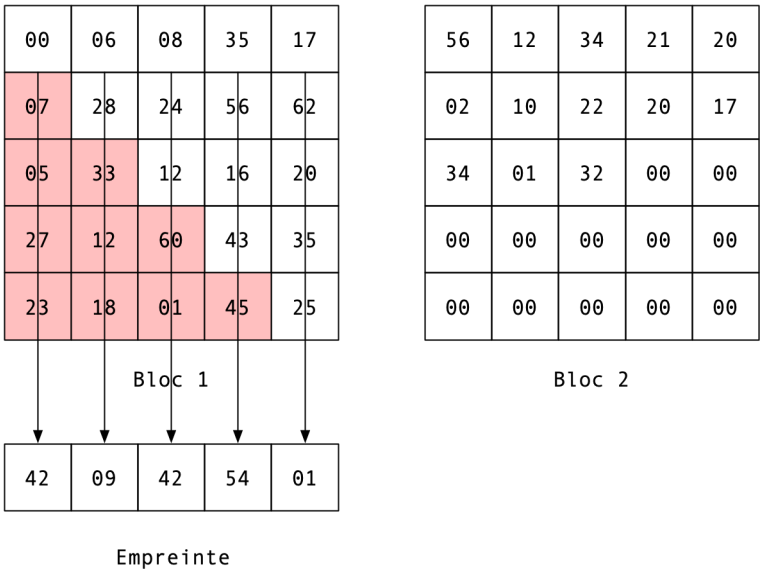
D) Calcul de l'empreinte pour le bloc en cours - étape 2

Chaque ligne du bloc en cours est décalée circulairement vers la gauche de son numéro d'indice. Rmq : l'indiçage commence à 0. Pour notre exemple on a :



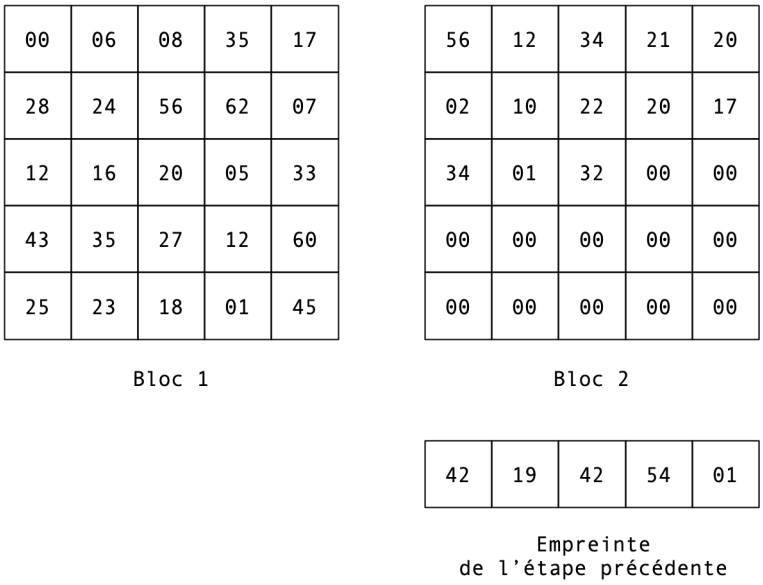
E) Calcul de l'empreinte pour le bloc en cours - étape 3

A l'instar de l'étape C), à l'empreinte courante est ajoutée la somme de chaque colonne en regard du bloc en cours. Ce cumul se fait modulo 64. Pour notre exemple, on a :



F) Passage au bloc suivant

S'il reste des blocs à traiter, aller à étape C) avec le bloc suivant. Pour notre exemple, on a :



3.1 Collisionnement de TTH_{64}^5 et preuve de travail

- A partir de la réponse établie à la question 2.2.1, donnez la fonction estimant la probabilité de collisionnement de TTH_{64}^5 avec une probabilité p.
- Quel sera l'effort à fournir pour générer un M tel que $TTH_{64}^5(M)$ débute par les valeurs 1 puis 2 puis 3 ?

3.2 Implémentation de TTH_{64}^5

Implémentez, dans le langage de votre choix - si possible en langage C - TTH_{64}^5

3.3 Collision de TTH_{64}^5

En vous basant sur l'algorithme de Floyd vu en cours, tentez de collisionner TTH_{64}^5. Autrement dit, fournissez, à l'aide de votre implémentation de la question précédente, 2 messages M_1 et M_2 t.q. $TTH_{64}^5(M_1) = TTH_{64}^5(M_2)$ avec $M_1 \neq M_2$