Introduction à la Cryptographie

TD2

1 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'exactly 256 bits.

1.1 ... 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 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 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 7950X¹. Poussé dans ses retranchements par l'overclocking, il atteint 293038 MIPS² 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*.

1. https://hwbot.org/hardware/processor/ryzen_9_7950x

2. Millions d'Instructions Par Secondes