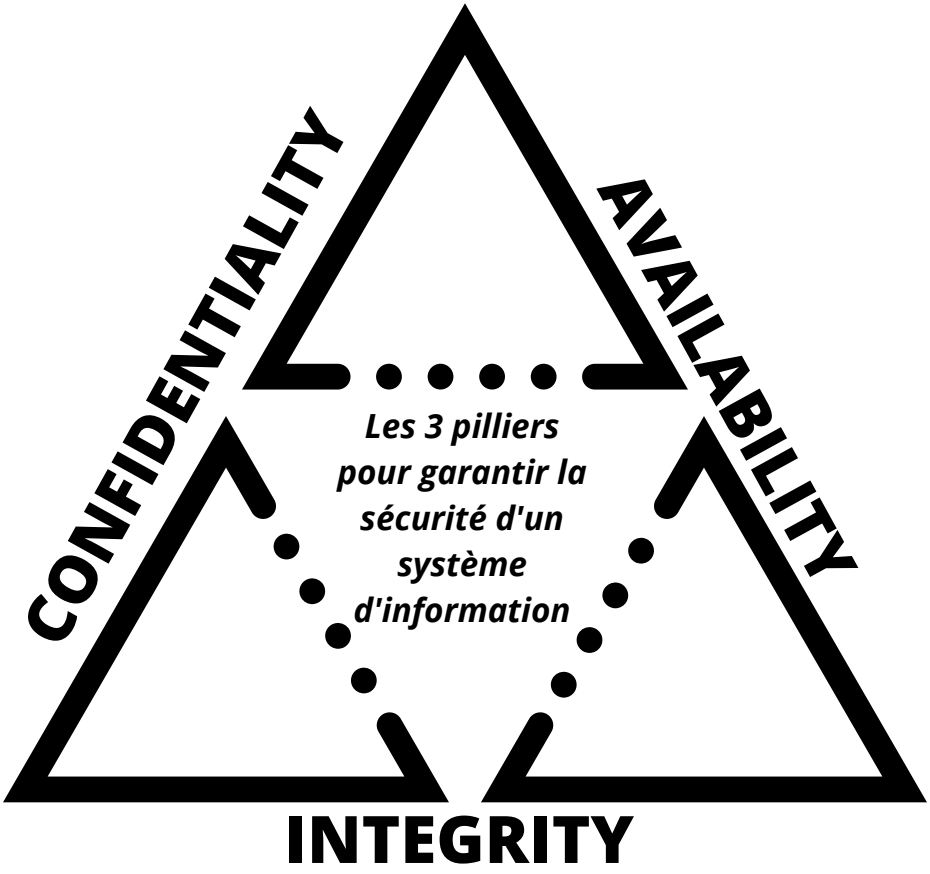
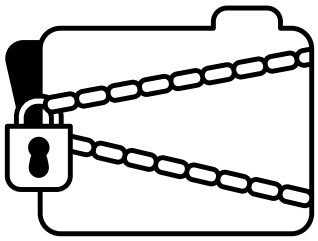
TRIADE CIA





Confidentialité

Il s'agit de garantir que seules les personnes autorisées peuvent accéder aux informations sensibles, en empêchant leur divulgation non autorisée à des tiers. Cela peut être effectuer par le choix de mots de passe "forts", en formant le personnel contre les attaques par ingénieurie sociale ou en chiffrant les données.

Intégrité

Cela implique que les données doivent être exactes, complètes et fiables, et qu'elles ne doivent pas être modifiées par des personnes non autorisées ou de manière non intentionnelle. Les mesures peuvent être des empreintes, des sommes de contrôle, des sauvegardes des données.

Disponibilité

Il est important de s'assurer que les données soient disponibles pour les personnes qui en ont besoin, lorsqu'elles en ont besoin, en protégeant contre les interruptions de service, les pannes de système et autres problèmes pouvant empêcher l'accès à l'information.

HACHAGE

Le hachage est une technique qui permet de transformer des données de taille arbitraire en une suite de caractère de taille fixe, appelé hash ou empreinte.

Propriétés

Déterministe

La fonction de hachage doit pour un message donnée, toujours donnée le même résultat.

Facile

Calculer le hash se fait "rapidement".

Résistante à la préimage

Très difficile de trouver à partir d'un hash, un message, tel que f(m) = h. C'est le prioncipe de fonction à sens unique (trapdoor function).

Résistante à la seconde préimage

Très difficile de trouver à partir d'un message, un second message ayant la même valeur de hash.

Résistante aux collisions

Très difficile de trouver deux messages différents ayant la même valeur de hash.

Effet avalanche

Une petite modification du message en entrée doit donner un hash très différent.

Utilisations

Intégrité

De la même manière que votre empreinte digitale est "unique" et vous identifie (1 chance sur 64 milliard d'en partager une), les fonctions de hachages peuvent servir à identifier un fichier, image, son, vidéo, transaction, etc....

Stockage de mot de passe

Les sites webs ne stockent pas vos de passe en clair, mais leur haché. Cela contribut à éviter que votre mot de passe soit compromis lors d'une intrusion sur les systèmes informatiques.

Générateur pseudo-aléatoire

Les fonctions de hachage ont une entropies très élévés ce qui rend les valeurs en sortie imprédictibles (~aléatoire). Il suffit de choisir une valeur de départ (seed), de calculer son hash (premier random), puis de calculer le hash du hash (deuxième random), etc...

Preuve de travail

La preuve de travail est un système utilisé pour sécuriser un réseau ou un processus informatique en utilisant la puissance de calcul. Elle est très utilisée dans la blockchain et permet de repousser des attaques telles que le déni de service et les spams.

Dériver des clés

La dérivation de clé est un mécanisme qui permet de calculer plusieurs clés à partir d'une valeur secrète comme un mot de passe ou une phrase secrète. Cela permet d'avoir plusieurs clés sans réduire la complexité du mot de passe initiale.

Table de hashage

En informatique, une table de hachage est une structure de donnée permettant de faire correspondre une clé avec une valeur. Cela permet de garder une recherche rapide, stockage efficace et un ajout et suppresion rapide.

DINER DES CRYPTOGRAPHES

Trois cryptographes dînent ensemble. À la fin de la soirée, le serveur leur annonce que le repas a déjà été payé. Ils ne savent pas qui a payé. Ils pensent que c'est soit l'un d'entre eux, soit la NSA. Les trois hommes veulent savoir si c'est la NSA. Mais, étant de nature discrète, ils ne veulent pas dévoiler non plus qui des trois à payer si c'est l'un d'eux.

Trouver une méthode pour résoudre leur problème

Indice 1

Chaque binôme doit partager un secret qui correspond à un bit.

Indice 2

L'opération xor est la base de ce protocole.
Pour rappel :
1 xor 1 = 0 0 xor 1 = 1
1 xor 0 = 1 0 xor 0 = 0

Indice 3

Chaque cryptographe va effectuer un calcul et annoncer le résultat, sauf celui qui a payé qui annonce l'inverse du résultat.

Solution

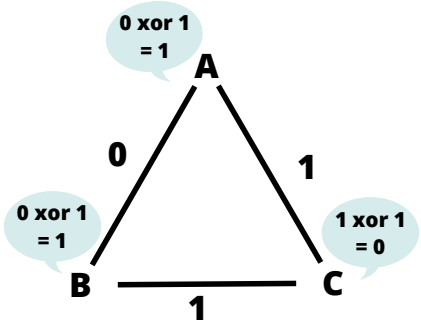
Chaque pair de cryptographe va partager un bit secret entre eux (choix libre). Maintenant, chaque cryptographe possède deux secrets (deux bits). Il suffit désormais que chacun en calcul le xor. Si ce n'est pas lui qui a payé, il annonce son résultat, sinon il annonce l'inverse du résultat.
Il suffit ensuite de faire un xor entre les trois annonces. Si le résultat est 0, alors la CIA a payé, sinon c'est un des cryptographes qui a payé.

Preuve : Soit k,l,m les secret entre A-B, B-C et C-A

Si aucun d'eux n'a payé : (k xor m) xor (k xor l) xor (l xor m)
= (k xor k) xor (l xor l) xor (m xor m)
= 0 xor 0 xor 0 = **0**

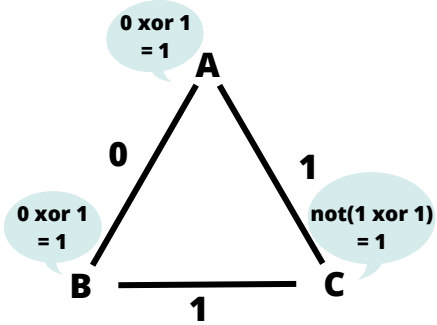
Si l'un d'eux a payé : (k xor m) xor ($\overline{\text{k xor l}}$) xor (l xor m)
= (k xor m) xor ($\overline{\text{k}}$ xor l) xor (l xor m)
= (k xor $\overline{\text{k}}$) xor (l xor l) xor (m xor m)
= 1 xor 0 xor 0 = **1**

Aucun des 3 n'a payé



1 xor 1 xor 0 = 0

L'un des 3 a payé (ici C)



1 xor 1 xor 1 = 1