Introduction au chiffrement et au hachage

Par Patrick Sentinel – 29a.ca

Allo les cyber aventuriers ! Dans le monde moderne, où nos données sont partout – des photos de vacances aux numéros de carte de crédit (eh oui, vos numéros de cartes de crédit sont probablement dans un dépôt de données 😬) – il n'est pas étonnant qu'on cherche à les protéger. C'est là qu'intervient le chiffrement, le super-héros discret des données, cachant nos informations aux yeux curieux comme une cape d'invisibilité numérique.

Le chiffrement : mais qu'est-ce que c'est ?

Imaginons un peu : vous avez une valise pleine de secrets, et vous voulez être certain que personne ne puisse la lire à moins d'avoir la clé. Le chiffrement, c'est cette serrure, et même plus que ça – c'est une série de verrous et de codes qui transforment le contenu en quelque chose d'illisible pour tout intrus. Une fois chiffrées, vos informations deviennent un ramassis de caractère pour tous… sauf pour ceux qui possèdent la clé 😊. C'est comme enfermer des informations dans une chambre blindée et que le seul moyen d'ouvrir la porte de la chambre est d'avoir une clé spéciale.

Évidemment, il existe plusieurs types de chiffrement, de ceux utilisés pour envoyer des messages entre espions pendant la guerre, à ceux qui protègent vos messages instantanés... Ce n'est pas l'alphabet de vos céréales du matin, mais bien des méthodes de chiffrement super puissantes qui transforment vos informations en un véritable casse-tête pour quiconque ne possède pas la bonne clé. Sans la clé, déchiffrer les informations devient presque impossible (évidemment tout dépend de l'algorithme utilisé).

Différence entre chiffrement et hachage

Aujourd'hui, on ne va pas s'alourdir de termes trop techniques mais vous devez conserver en mémoire deux expressions :

1- Chiffrement : processus par lequel des informations lisibles sont transformées en une version non lisible qu'on appelle le *cipher* ou chiffré. Cette transformation s'effectue à l'aide d'un algorithme de chiffrement et d'une clé. Le processus est **RÉVERSIBLE**.
2- Hachage : processus par lequel des informations lisibles sont transformées en une version non lisible qu'on appelle *hash* ou empreinte de hachage. Contrairement au chiffrement, le hachage est **IRRÉVERSIBLE**.

Dans un des prochains articles, j'irai plus en profondeur dans les explications du chiffrement et du hachage mais pour le moment on reste à la surface 😊.

Le *cipher* : la recette secrète

Un chiffrement, c'est un peu comme une recette secrète pour conserver vos données sous clé. Grâce à une méthode ou un algorithme, il transforme des informations parfaitement lisibles en un charabia incompréhensible... sauf, bien sûr, pour ceux qui détiennent la fameuse clé magique ! Sans cette clé, même les espions les plus chevronnés risquent de rester perplexes, à moins qu'ils aient des années devant eux pour tenter de deviner la recette.

Ainsi, sans la clé, il est **théoriquement (avec certaines nuances)** impossible de déchiffrer le texte chiffré !

Le *hash* : l'irréversible!

Le hachage est souvent la technologie utilisée pour stocker vos mots de passe dans les bases de données 😊. Le hachage est, en principe, impossible à remettre en clair ! Oui, vous avez bien lu : lorsqu'une suite de caractères est hachée, il devrait être impossible d'appliquer une fonction inverse pour la retrouver dans son état d'origine. Plutôt cool, non ? Bien entendu, cela dépend de l'algorithme de hachage, et il y a aussi des nuances que je ne vais pas aborder ici !

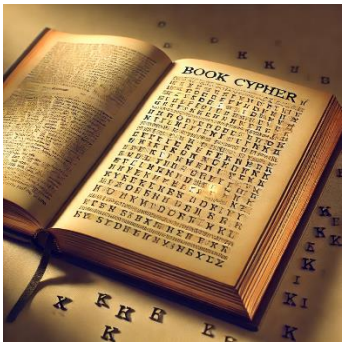
Par exemple, si on utilise un algorithme de hachage assez populaire tel que SHA256 et qu'on veut hacher les mots suivants : « Bonjour followers » alors le résultat sera :

« a33971b80e508247af0dccc39a2f7b5a7b678d265b8b9bb9dd7430e2c5175bed »

Alors, ça ne ressemble plus du tout aux mots de départ, n'est-ce pas ? Parfait ! C'est exactement le boulot du hachage : transformer vos infos en quelque chose de totalement méconnaissable, un peu comme si on passait votre texte dans un blender numérique. Imaginez vos mots de passe transformés en un cocktail incompréhensible de chiffres et de lettres. Normalement, ces informations sensibles devraient être soigneusement hachées puis stockées dans une base de données elle-même chiffrée, histoire de doubler les verrous! Parce que oui, vos données, c'est sacré, et mieux vaut les garder bien protégées – un peu comme le secret de votre recette de grand-mère ! 😄

Le *Book Cipher* : quand les livres deviennent des clés

Maintenant que vous savez ce qu'est un *cipher* et un *hash* sur les bases du chiffrement, explorons le *Book Cipher*, qui est vraiment *old-school*. Imaginez que vous et un ami avez le même livre sur votre étagère, disons, un classique comme « *Le Petit Prince* ». Vous décidez que, pour chaque message, vous allez utiliser des numéros pour représenter la page, la ligne, et le mot sur cette ligne pour composer un message chiffré.



Prenons l'exemple d'un *Book Cipher* en action. Imaginons que vous vouliez dire à un ami: "Allons au restaurant samedi". Vous pourriez utiliser des numéros pour chaque mot, tels que 3:12:4 pour la **page 3, ligne 12, quatrième mot de la ligne**. Seule la personne ayant le livre « *Le Petit Prince* » **et le cipher exacte peut déchiffrer votre message**. Voilà un secret bien gardé, caché entre les lignes!

Autre exemple : si vous recevez le message : 3:13:6 6:2:8 34:18:6 20:28:8

Ça voudrait dire que :

- Le premier mot se trouve à la page 3, ligne 13 et c'est le 6e mot de la phrase;
- Le deuxième mot ce serait page 6, ligne 2 et le 8e mot de la phrase;
- Le troisième mot ce serait page 34, ligne 18 et le 6e mot;
- Finalement pour le dernier mot ce serait page 20, ligne 28 et le 8e mot de la phrase.

Ensuite, il ne vous reste qu'à mettre les mots ensemble pour obtenir une signification, facile mais il faut savoir de quel livre on parle sinon on peut chercher longtemps…

Pourquoi le chiffrement est-il important ?

Le chiffrement, c'est un peu comme accrocher des rideaux chez soi : ça protège votre vie privée. Sans lui, n'importe qui pourrait lire vos messages, accéder à vos photos, ou même trouver vos informations bancaires 😟. Chaque fois que vous envoyez un message ou partagez une information sensible en ligne, il y a de fortes chances que le chiffrement soit derrière, transformant votre message en code pour le rendre illisible.

Le *Book Cipher*, quant à lui, fait partie des *ciphers* dits "symétriques" et vieux. Il est amusant et même légèrement romantique – après tout, qui n'a pas rêvé d'envoyer des messages secrets comme dans les romans d'espionnage ?

En conclusion : l'art de l'invisible

Vous avez peut-être tout un tas de questions portant sur le hachage et le chiffrement. Pas de panique, on va aborder tout ça dans d'autres articles. Celui-ci n'est qu'une introduction, et je ne veux pas vous noyer sous les informations 😊. Comme on dit, chaque chose en son temps.

Le chiffrement, dans toutes ses formes, est l'art de rendre l'important non lisible à tous. Que ce soit pour protéger des secrets d'État ou simplement pour s'amuser à ce que vos messages restent privés entre vous, les *ciphers* sont des alliés puissants. Et, qui sait, peut-être que le prochain message secret que vous enverrez sera caché dans les pages d'un livre que vous partagez avec un complice de confiance. Alors, choisissez bien votre livre et rappelez-vous: parfois, les secrets les mieux gardés sont ceux qui se cachent entre les lignes 😉.