**Fonctions de Hachage et sécurité**

1. **Fonction de hachage**

Une fonction de hachage H accepte un bloc de données de longueur variable M en entrée et produit une valeur de hachage de taille fixe h = H(M). Une "bonne" fonction de hachage a la propriété que les résultats de l'application de la fonction à un grand ensemble d'entrées produiront des sorties qui sont distribuées de manière égale et apparemment aléatoire. En général, l'objet principal d'une fonction de hachage est d’assurer l'intégrité des données. Une modification d'un ou plusieurs bits de M entraîne, avec une forte probabilité, une modification de la valeur de hachage.

Le type de fonction de hachage nécessaire aux applications de sécurité est appelé *Fonction de Hachage Cryptographique ou FHC*. Une FHC est un algorithme pour lequel il n’est pas possible, au travers des ressources calculatoires actuelles, (Car aucune attaque n'est significativement plus efficace que la force brute) de trouver soit :

1. Un bloc de données qui correspond un à résultat de hachage prédéfini (propriété unidirectionnelle),
2. Deux blocs de données qui correspondent au même résultat de hachage (propriété sans collision).

En raison de ces caractéristiques, les fonctions de hachage sont souvent utilisées pour vérifier l’intégrité des données (Données ayant ou non subi des modifications).

En général, l'entrée est complétée par un entier multiple d'une longueur fixe (par exemple, 1024 bits), et le remplissage comprend la valeur de la longueur du message original en bits. Le champ de la longueur est une mesure de sécurité destinée à augmenter la difficulté pour un attaquant de produire un autre message avec la même valeur de hachage.

1. Application des Fonctions de Hachage en Cryptographie

L'algorithme cryptographique le plus polyvalent est la fonction de hachage cryptographique. Elle est utilisée dans une grande variété d'applications de sécurité et de protocoles Internet. Pour mieux comprendre certaines des exigences et des implications en matière de sécurité des fonctions de hachage cryptographiques, il est utile d'examiner l'éventail des applications dans lesquelles elles sont employées.

**Authentification des messages** : L'authentification des messages est un mécanisme ou un service utilisé pour vérifier l'intégrité d'un message. L'authentification des messages garantit que les données reçues sont exactement celles envoyées (c'est-à-dire qu'il n'y a pas eu de modification, d'insertion, de suppression ou de relecture). Dans de nombreux cas, il est nécessaire que le mécanisme d'authentification garantisse que l'identité présumée de l'expéditeur est valide. Lorsqu'une fonction de hachage est utilisée pour fournir une authentification de message, la valeur de la fonction de hachage est souvent appelée *condensé* de message.

Le mécanisme d'utilisation d'une fonction de hachage pour l'intégrité des messages est la suivante. L'expéditeur calcule une valeur de hachage en fonction des bits du message et transmet à la fois la valeur de hachage et le message. Le récepteur effectue le même calcul de hachage sur les bits du message et compare cette valeur avec la valeur de hachage reçue.

En cas de différence, le récepteur déduit que le message (ou éventuellement la valeur de hachage) a été modifié (figure 11.2a). La valeur de hachage doit être transmise de manière sécurisée. En d'autres termes, elle doit être protégée de telle sorte que si un adversaire modifie ou remplace le message, il ne puisse pas modifier également la valeur de hachage pour tromper le récepteur. Ce type d'attaque est illustré à la figure 11.2b. Dans cet exemple, A transmet un bloc de données et joint une valeur de hachage. D intercepte le message, modifie ou remplace le bloc de données, calcule et joint une nouvelle valeur de hachage. B reçoit les données modifiées avec la nouvelle valeur de hachage et ne détecte pas le changement. Pour empêcher cette attaque, la valeur de hachage générée par Alice doit être protégée.

La Figure suivante illustre diverses façons d'utiliser un code de hachage pour fournir une authentification de message, comme suit.

a. Le message plus le code de hachage concaténé sont chiffrés à l'aide d'un chiffrement symétrique. Comme seuls A et B partagent la clé secrète, le message doit provenir de A et n'a pas été modifié. Le code de hachage fournit la structure ou la redondance nécessaire à l'authentification. Le cryptage étant appliqué à l'ensemble du message et au code de hachage, la confidentialité est également assurée.

b. Seul le code de hachage est crypté, à l'aide d'un cryptage symétrique. Cela réduit la charge de traitement pour les applications qui ne nécessitent pas de confidentialité.









Exemples simplifiés d’utilisation des focntions de Hashing pour message authentification.

1. **Caractériqtiques d’une Fonction de Hachage**

|  |  |
| --- | --- |
| **Caractéristique** | **Description** |
| Entrée de taille variable | H peut être appliqué à un bloc de données de n'importe quelle taille |
| Sortie de taille fixe | H produit une sortie de longueur fixe**.** |
| Efficacité | H(x) est relativement facile à calculer pour tout x donné, ce qui rend pratique les implémentations matérielles et logicielles. |
| Propriété de sens unique | Pour toute valeur de hachage h donnée, il est calculatoirement infaisable de trouver y tel que H(y) = h. |
| Resistance faible aux collisions | Pour tout bloc donné x, il est calculatoirement infaisable, de trouver y ≠ x tel que H(y) = H(x). |
| Resistance forte aux collisions | Il est calculatoirement infaisable de trouver une paire quelconque (x, y) avec x ≠ y, telle que H(x) = H(y). |
| Caractère Pseudo aléatoire | La sortie de H répond aux tests standards pseudo-aléatoires |