CRYPTOGRAPHIE (1)

CRYPTOGRAPHIE (definition)
La cryptographie est une methode pour proteger des informations considerEs comme sensibles en utilisant des codes secrets ou cles de chiffrement de sorte que seuls les destinataires puissent les lire et les traiter.

CRYPTOGRAPHIE (objectif)
Le but de la cryptographie vise a proteger des informations ou donnees sensibles des personnes qui ne sont pas autorisEes a les consulter en rendant les informations totalement incomprehensible afin de preserver la confidentialitE.

LES 4 FONCTIONS DE LA CRYPTOGRAPHIE (services offerts)
- ConfidentialitE: assure que les donnees ne peuvent pas etre consulter que par les personnes autorisEes
- IntegritE: assure que les donnees ne sont pas modifiEs depuis l'envoi
- Authentification/Identification: prouver l'origine des donnees et l'identitE d'une personne
- Signature proprement dite (undeniability ou non-repudiation): permet a une personne de prendre part a un contrat avec impossibilitE de renier ensuite ses engagements

CHIFFREMENT CLASSIQUE (2 techniques)
- Chiffrement par substitution: chiffrement par lequel chaque caractere d'un text en clair est remplacE par une autre caractere dans le texte chiffrE
- Chiffrement par transposition: chiffrement par lequel tout les caracteres d'un text en clair demeurent inchangEs mais dont les positions respectives sont modifiEes

INCONVENIENTS DU CHIFFREMENT CLASSIQUE
Les techniques de chiffrement classiques presentent comme faille la limitation du nombre de cle et de permutation

EXEMPLES DU CHIFFREMENT CLASSIQUE
- Chiffre de Jules Cesar
- Chiffrement par substitution
- Chiffrement par transposition

PRINCIPE DU CHIFFREMENT A CLE SECRETE
- Consiste a utiliser la meme cle pour le chiffrement et le dechiffrement
- Facile a utiliser mais moins securisE
- Necessite une methode sure pour transferer une cle secrete d'une partie a une autre

CRYPTOGRAPHIE (2)

LES 2 METHODES DE BASE D'ALGORITHMES A CLE SECRETE
- Algo de chiffrement en continu: operent sur un message en clair par un bit ou un octet a la fois
- Algo de chiffrement par blocs: operent sur un message en clair par des groupes de bits appelEs blocs

INCONVENIENTS DES CHIFFREMENTS A CLE SECRETE
- Peut etre percE par une attaque a force brute ou brute force en anglais, cette technique est utilisEe dans le cryptanalyse pour trouver un mot de passe ou une cle en testant divers combinaisons possibles jusqu'a trouver la bonne combinaison.
- Il faut n(n−1)/2 cles secretes pour assurer une communication en toute securitE
- Il faut un canal secret pour transmettre la cle secrete
- Il n'assure que la confidentialitE mais pas l'authenticitE et la non−repudiation

CHIFFREMENT SYMETRIQUE (exemple de cryptosysteme a cle secrete)
- Chiffrement de Vienman
- IDEA
- AES
- DES
- RC4

PRINCIPE DU CHIFFREMENT A CLE PUBLIQUE
- Utilise une cle pour le chiffrement et une autre cle pour le dechiffrement
- On peut publier la cle publique tout en conservant la cle privEe en secrete
- BasE sur une methode mathematique complexe garantissant un encryptage facile et rapide et un decryptage difficile

BASE D'ALGORITHME DE CHIFFREMENT A CLE PUBLIQUE
- Concus de telle maniere a ce que la cle de chiffrement soit differente de la cle de dechiffrement
- De plus la cle de dechiffrement ne peut pas etre calculEe a partir de la cle de chiffrement
- De tels algorithmes sont appelEs "algorithmes a cle publique" car la cle de chiffrement peut etre rendue publique

INCOVENIENTS DES CHIFFREMENTS A CLE PUBLIQUE
- Il peut avoir un temps de calcul considerable en CPU pour traiter un encryptage et un decryptage asymetrique par rapport au chiffrement symetrique
- Il n'est pas reservE au cryptage de masse en raison de son utilisation des ressources elevEs
- Il peut etre percE si la cle privEe n'est pas en securitE

EXEMPLES DES CHIFFREMENTS A CLE PUBLIQUE
- Diffie−Hellman
- ECC
- El Gamal
- DSA
- RSA

CRYPTOGRAPHIE (3)

HACHAGE (definition)
Le hachage consiste a transformer une chaine de caractere en une valeur a longueur fixe, generalement plus courte et representant la chaine d'origine. Il est notamment utilisE pour indexer un element dans une base de donnEes, en effet, il est plus rapide de recuperer une valeur a partir d'une cle de hachage reduite plutot qu'a l'aide de sa valeur d'origine

MD5 (Message Digest 5)
C'est une fonction de hachage cryptographique developpE par Rivest en 1991 qui calcule a partir d'un fichier numerique, son empreinte numerique en l'occurence une sequence de 128 bits ou 32 caracteres en hexadecimal avec une forte probabilitE que 2 fichiers differents donnent 2 empreintes numeriques differentes

SHA (Secure Hash Algorithm)
C'est une fonction de hachage qui utilise la norme SHS (Secure Hash Standard) de la norme du gouvernement americain

CRYPTOSYSTEME HYBRIDE (definition)
Le cryptosysteme hybride combine la comiditE d'un chiffrement asynchrone et l'efficacitE d'un chiffrement synchrone. Les chiffrements asynchrones sont pratiques de ce fait qu'ils n'exigent pas que l'expediteur et le destinataire se partagent un secret commun pour communiquer en toute securitE. Cependant, ils se reposent sur des calculs mathematiques compliquEs et sont donc moins efficace par rapport a un cryptosysteme symetrique comparable.

CRYPTOSYSTEME HYBRIDE (exemple)
- GPG (GNU Privacy Guard)
- PGP (Pretty Good Privacy)

DIFFERENCES ENTRE CHIFFREMENT SYMETRIQUE ET ASYMETRIQUE

Chiffr. Symetrique	Chiffr. Asymetrique
Il ne nécessite qu'une seule clé pour le chiffrement et le déchiffrement	Il nécessite deux clés, une clé publique et une clé privée, un pour chiffrer et l'autre pour déchiffrer.
La taille du texte chiffré est identique ou inférieure à celle du texte brut d'origine.	La taille du texte chiffré est identique ou superieur à celle du texte brut d'origine.
Demande un canal secret pour envoyer la cle secrete	Aucun canal secret n'est necessaire pour pratiquer l'echange de la cle publique.
Le processus de cryptage est très rapide (faible utilisation des ressources)	Le processus de cryptage est lent (utilisation des ressources elevEs)
La longueur de clé utilisée est de 128 ou 256 bits	La longueur de la clé utilisée est de 2048 ou plus
Il est utilisé lorsqu'une grande quantité de données doit être transférée	Il est utilisé pour transférer de petites quantités de données
Il ne fournit que la confidentialité	Il assure la confidentialité, l'authenticité et la non-répudiation
Il faudrait n(n-1)/2 cles secretes pour assurer la communication	2n cles seulement sont necessaires pour que n entitEs communiquent en toute securitE
Peuvent etre percés par une attaque par "force brutale"	Ne peuvent etre percés tant que la cle privée est en securitE