



Cryptographie

Concepts de la cryptographie





Votre instructeur

Thierry DECKER
mail@thierry-decker.com

Cryptographie Concepts

Sommaire

- Le domaine général CRYPTOLOGIE
 - Deux Branches
 - Cryptographie : art du chiffrement possession de la/les clé(s)
 - Cryptanalyse : art du déchiffrement sans possession de la/les clé(s)

Cryptographie Concepts

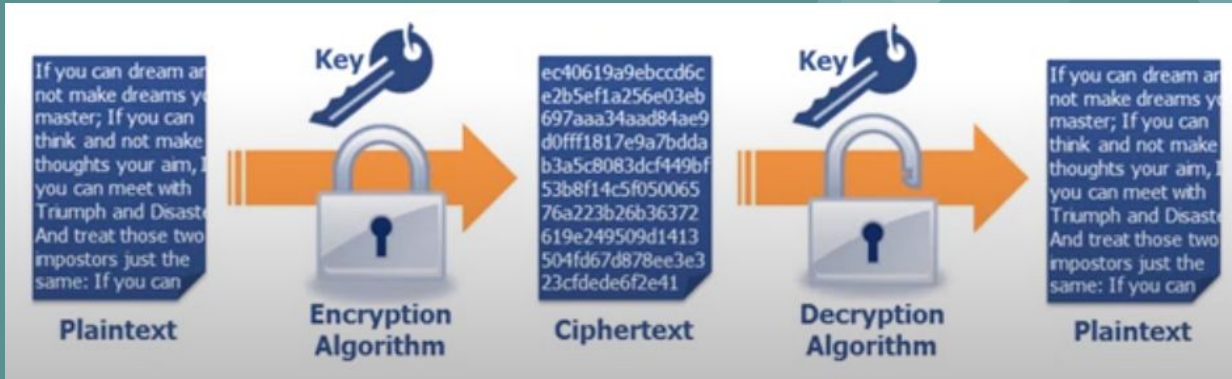
Sommaire

- Survol de la cryptographie
- Chiffrement symétrique vs asymétrique
- Signature digitale
- Non-répudiation
- Méthodes de chiffrement et déchiffrement
 - Chiffrement par bloc
 - Chiffrement de flux
 - Cryptographie à courbe elliptique (ECC) -> “Crypto Monnaies”
 - Cryptographie quantique (Suprémie Quantique)
- Hachage cryptographique
- Stéganographie
- Utilisation de technologies éprouvées

Cryptographie Concepts Survol

- Qu'est-ce que la cryptographie ?
 - Science et étude de la dissimulation de l'information
 - Cacher l'information en la convertissant d'un texte clair en un texte chiffré (Chiffrement)
 - Puis d'un texte chiffré en un texte en clair (déchiffrement)

Cryptographie Concepts Survola



- Algorithmes publics connus
- Longueur de clé définissant la robustesse du chiffrement
- La clé ne doit pas pouvoir être déduite du texte chiffré (dans un temps raisonnable)
- Le texte en clair ne doit pas pouvoir être déduit du texte chiffré sans avoir la clé (dans un temps raisonnable)

Cryptographie Concepts

Survol

- Bénéfices de la cryptographie
- Confidentialité
 - Protéger l'information en transit
 - Protéger l'information stockée
- Non-répudiation et authentification
 - Un message chiffré avec votre clé privée ou signé avec votre signature numérique vient forcément de vous

Cryptographie Concepts Survol

- Bénéfices de la cryptographie
- Contrôle d'accès
 - Avec le chiffrement symétrique, seul le ou les détenteur(s) de la clé secrète peut déchiffrer le message
 - Avec le chiffrement asymétrique, un certificat numérique peut être utilisé pour l'authentification et donc le contrôle de l'accès au message
- Intégrité
 - Les résumés de messages (Message Digest) peuvent-être utilisés pour savoir si le message a été trafiqué pendant son transport ou depuis le calcul du dernier résumé

Cryptographie Concepts Survол

- Comment la cryptographie fonctionne-t-elle ?
- Un “chiffre” est une paire d’algorithme de chiffrement et de déchiffrement
- Un chiffre et une/des clé(s)
 - Un algorithme chiffre le message en lui appliquant une clé
 - Un autre algorithme déchiffre le message en lui appliquant une clé
- Certains algorithmes sont plus forts que d’autres
- De longues clés font un chiffrement plus fort
 - Des clés de 40 bits ne sont pas sûres
- Chiffres classiques
 - Chiffres de rotation ou décalage (Caesar)
 - Chiffres de transposition (permutation) “Vigenere” (apporte de la diffusion)

Cryptographie Concepts Survoll

Caesar Substitution Cipher




Diagram illustrating the Caesar Substitution Cipher (ROT6) mapping:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕	↕
G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

Plaintext: asparagus
Ciphertext: gyvgxgmay

Cryptographie

Symétrique vs Asymétrique

- Chiffrement Symétrique
 - La même clé est utilisée pour le chiffrement et le déchiffrement
 - La gestion des clés est le principal problème
 - Garder la clé secrète (distribution des clés)
 - Partager de façon sûre la clé
 - Généralement plus rapide que le chiffrement asymétrique seul
 - La force du chiffrement est affecté par :
 - La longueur de la clé
 - Nombre d'itération au travers de l'algorithme
 - “Potentiellement” vulnérable aux attaques en force brute
 - Changement régulier de clé pour pallier à cette vulnérabilité

Cryptographie

Symétrique vs Asymétrique

- Chiffrement Asymétrique
 - Une paire de clés (mathématiquement liées) est utilisée :
 - Une clé pour chiffrer
 - Une autre clé pour déchiffrer
 - Une clé est accessible publiquement (clé publique)
 - L'autre clé doit rester secrète (clé privée)
 - Chaque clé peut chiffrer ou déchiffrer
 - Chiffrer à l'aide de la clé publique, déchiffrer avec la clé privée
 - Chiffrer à l'aide de la clé privée, déchiffrer avec la clé publique
 - Une des deux clés ne peut être utilisée pour chiffrer et déchiffrer

Cryptographie

Signature numérique

- Chiffrement asymétrique utilisé
- Permet de signer des données ou des messages
- Fournit l'authenticité, la non-répudiation et l'intégrité
- Confirme que les données ou le message reçu proviennent bien de celui qui prétend en être l'émetteur des données ou du message

Cryptographie

Non-répudiation

- S'assurer que l'auteur du message ne puisse réfuter plus tard le fait d'en avoir été à l'origine
- Le chiffrement asymétrique permet de mettre en place cette sécurité
- Seule la clé privée a pu être utilisée pour chiffrer ou signer un message
- Possibilité d'ajouter des services de non-répudiation dans le chiffrement ou la signature numérique
 - Preuve de l'origine
 - Preuve que l'information a été reçue et bien correctement reçue (intégrité)
- Ne prend pas en compte l'accès physique non autorisé
 - Envoyer un message depuis le poste de travail d'un tiers
 - Ne fonctionne que si la clé privée reste privée

Cryptographie

Chiffrement par bloc

- Chiffrement symétrique
- Les messages sont découpés en blocs de longueur fixe et chiffrés individuellement
- Généralement des blocs de 64 ou 128 bits
- Si le dernier bloc est plus court, du bourrage est ajouté (zéros, uns ou des patterns plus complexes selon l'algorithme)
- Chaque bloc chiffré à la même longueur que le bloc non chiffré
- La robustesse est liée à la non réutilisation des clés

Cryptographie

Chiffrement par bloc

- La robustesse est liée à la non réutilisation des clés
- Si deux ou plusieurs blocs sont chiffrés avec la même clé, un attaquant à une chance de les comparer et de casser le chiffrement
- Un bon bloc chiffré ne doit pas permettre à un attaquant de déduire la clé
- Peu de changement sur un bloc doit provoquer un grand changement sur le résultat du chiffrement
- Plus lent que le chiffrement de flux

Cryptographie

Chiffrement de flux

- Chiffrement symétrique
- Un flux continu de bits/octets est chiffré, un bit/octet à la fois
- Plus rapide, utilisant moins de ressources que le chiffrement par bloc
- Des générateurs d'espaces de clé pseudo-aléatoires sont utilisés
- Ces espaces de clés se répèteront éventuellement
 - Plus la période sera longue et plus le chiffrement sera robuste

Cryptographie

Cryptographie à courbe elliptique (ECC)

- Chiffrement asymétrique
- Permet un chiffrement asymétrique plus rapide et plus robuste avec des clés plus courtes
- Design mathématique compact
- Utilise des courbes elliptiques à la place d'entiers comme clés
- Utilisé dans de nombreuses variantes utilisable notamment des les appareils mobiles possédant peu de ressources de traitement

Cryptographie

Cryptographie quantique



- Utilise la physique en lieu et place des mathématiques
- Concept émergent et coûteux, toujours en recherche
- Le principe est que lorsque nous mesurons l'information, nous perturbons cette information
 - Lorsque l'on observe des photons polarisés, nous changeons leur polarisation
 - Lorsque l'on mesure la température de l'eau, nous changeons la température de l'eau en introduisant un thermomètre
- La cryptographie quantique permet de dire que l'information a été espionnée ou non pendant son transport
 - En polarisant un photon dans une direction pour zéro et une autre direction pour 1
 - Si quelqu'un espionne ces données, la polarisation sera changée
- Une implémentation est QKD (Quantum Key Distribution)

Cryptographie

Hachage cryptographique

- Ni un chiffrement, ni un déchiffrement
- Le hachage crée une valeur qui est le résumé ou le “digest” d’un message
- Deux messages ne peuvent pas créer le même “hash” lorsqu’ils sont traités pas le même algorithme
- Deux messages peuvent avoir le même “hash” si la clé est courte ou qu’un attaquant utilise une attaque de collision
- Algorithme à sens unique
 - On ne peut obtenir le texte clair à partir de son “hash” même avec la clé

Cryptographie

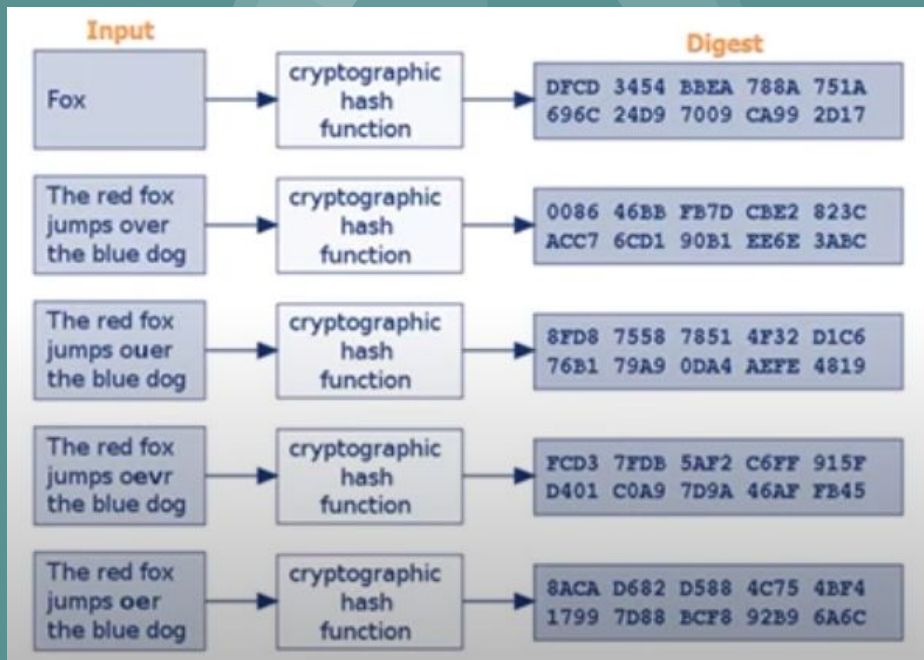
Hachage cryptographique

- Utilisé pour l'intégrité : Si l'information est modifiée alors le "hash" sera différent
 - Message Digest
 - Signature numérique
 - Message Authentication Codes (MAC)
- Utilisé pour le stockage des mots de passe
 - Stockage sûr
 - Vérification : Le "hash" du mot de passe entré doit être identique au "hash" stocké
 - Un mot de passe ne peut donc pas être retrouvé, seulement réinitialisé
 - Le mot de passe de l'utilisateur n'est jamais stocké

Cryptographie

Hachage cryptographique

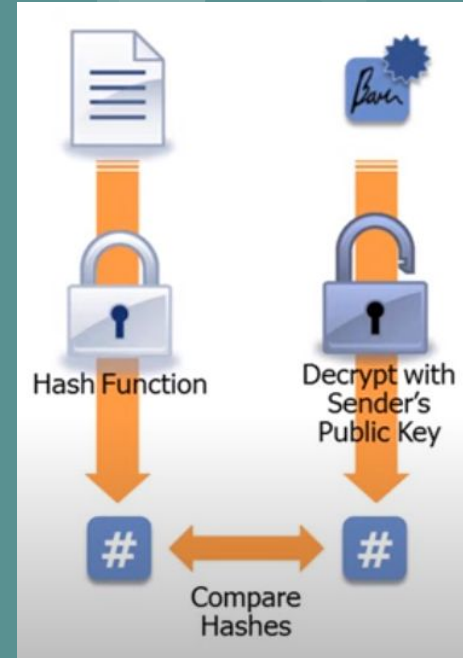
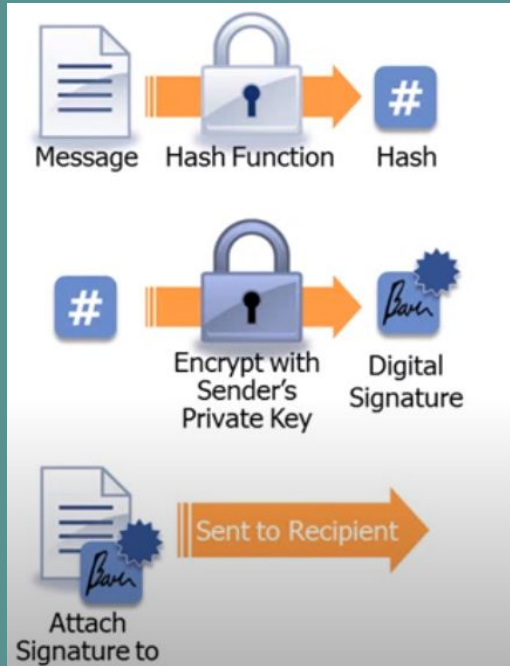
- Une fonction mathématique qui prend n'importe quel message de n'importe quelle longueur et retourne une suite de bits de longueur fixe



Cryptographie

Hachage et signatures numériques

- Intégrité et non-répudiation



Cryptographie

Chiffrement de transport

- Le chiffrement est également utilisé pour protéger les transmissions au travers des réseaux publics
 - VPN :
 - IPSec
 - OpenVPN
 - Communications entre Navigateurs et Serveurs Web
 - TLS/SSL
 - HTTPS
 - Transferts de données et gestion à distance
 - SSH
 - SCP
 - SFTP
 - etc.

Cryptographie

Chiffrement de transport

- TLS, par exemple, utilise à la fois le chiffrement asymétrique et symétrique
- Le chiffrement asymétrique pour échanger une clé secrète
- Le chiffrement symétrique pour le transfert de données chiffrées à l'aide de la clé secrète échangée

Cryptographie

Stéganographie

- Cacher ou embarquer un message dans un autre
- Comme écrire un message secret avec de l'encre invisible et...
- Ecrire un texte en clair par dessus
- L'objectif est de ne pas attirer l'attention
- Le message peut être caché dans une image, un fichier audio ou vidéo
 - Une méthode pour les images est d'utiliser le dernier bit du code couleur de chaque pixel pour cacher l'information
 - On peut également chiffrer les données avant ou après que le message ait été caché...

Cryptographie Stéganographie

- Appelé parfois “Electronic Watermarking” quand une image est ainsi labellisée afin d’éviter le piratage
- Des outils sont disponibles
- Souvent utilisés pour des activités illicites (vol de données ou dans des pays où le chiffrement est interdit)

Cryptographie

Technologies éprouvées

- N'utiliser que des algorithmes qui, à ce jour, sont considérés comme "forts"
 - Penser au compromis entre sécurité, vitesse et facilité de mise en place
- Se tenir informé des nouveautés de la cryptographie
 - Par le passé, des algorithmes largement utilisés ont été "cassés" (WEP, MD5, etc.)
 - De nouvelles méthodes apparaissent régulièrement
- Tirer parti d'un chiffrement fort avec une bonne gestion des clés



Cryptographie - Q&A

Merci de votre attention !