Licence 2ème Année

V. Pagé
(google vpage)

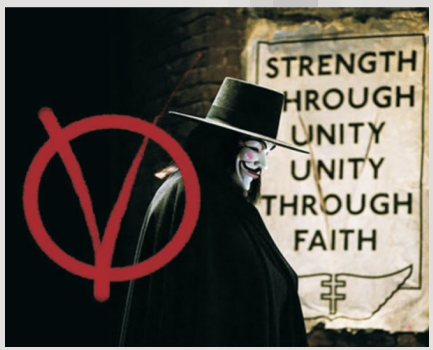
Sécurisation des données :

Cryptographie et stéganographie

Objectifs du cours

Introduction à la Cryptographie :

Notions de Stéganographie :



Image

Cachée

Premiere Partie :

Introduction à la Cryptographie

Cryptographie : Introduction

Historiquement : Objectifs militaires
Chiffrer les ordres militaires
- dès l'antiquité : code de César decalage de lettres de 3
  (A-> D …)
- Renaissances : travaux mathématiques
- 2ème guerre mondiale : Enigma
=> Lire « Histoire des codes secrets » (S. Singh)

Aujourd'hui : Objectifs civils
- paiement en ligne
- protection de la vie privée

Cryptographie : Introduction 2

Principe général :

La sécurité des données chiffrées ne dépend pas de la méconnaissance de la méthode de chiffrement.

La méthode doit être connue. Le secret réside dans une « clef »

Ceci permet de tester la robustesse de la méthode aux attaques...

Codage des données en Bits

Problèmes du chiffrement de César :
- Facile a casser.
- Ne fonctionne que pour des textes.

Pour le dernier point : Tout donnée numérique est, par définition, un ensemble de bits.

Eventuellement, ces bits peuvent être vus comme des nombres (1, 2,4, ou 8 octets) pour faire des opérations mathématiques.

=> permet de traiter tout type de fichier de façon identique.

I. Cryptographie Symétrique

Principe : Une clef identique pour chiffrer, déchiffrer.
Notation : Ks, la clef secrète

On prend un texte « en clair ».
On le chiffre avec la clef secrète (et une fonction de chiffrement).
On le déchiffre avec la clef secrète (et une fonction de déchiffrement).

Tchiffré = C(Tclair, Ks)

Tdéchiffré = D(Tchiffré, Ks)

Comme on veut Tdéchiffré = Tclair, il faut $D = C^{-1}$

Le XOR

La fonction de base de la cryptographie symétrique est le XOR :
Sur un bit, cette fonction a la table de vérité suivante :

Clair	Clef	Chiffré = Clair XOR Clef
0	0	0
1	0	1
0	1	0
1	1	0

$$X = 0 \Rightarrow Z = X \; xor \; Y = Y$$

$$X = 1 \Rightarrow Z = X \; xor \; Y = \overline{Y}$$

Déchiffrement : XOR aussi, car (Chiffré xor Clef = Clair).
Démontrez le.

Le One Time Pad

Sur un Bit, sans connaissance du bit correspondant a la clef, nous sommes incapable de connaître le bit correspondant au message.

D'ou la technique de chiffrement suivante pour chiffrer un message de n bits :

- On génère aléatoirement une clef de n bits
- On chiffre le message bit a bit (clair xor Clef)

Le message est rigoureusement indéchiffrable sans la clef.
(selon la légende, c'est le chiffrement existant, pendant la guerre froide, entre Moscou et Washington).

Reste a transmettre la clef...

Le One Time Pad 2

Problèmes : Pour communiquer, Alice et Bob doivent d'abord disposer de clefs de taille suffisante pour chiffrer les messages qu'ils devront échanger.

Comment adapter cela ? On peut imaginer une clef de taille fixe (disons 256 octets et un xor par bloc sur les messages).

Le problème est alors que la clef ressert. Il est souvent facile de casser ce chiffrement si l'on sait des choses sur le contenu des messages echangés (exemple : les messages sont des pages Web).

=> Adaptations plus sûres (DES, triple DES...) et Changer de clef !

Le One Time Pad 3

Algorithme merveilleux : Simple, rapide, le plus fiable au monde.

MAIS : Comment mettre cela en œuvre ?
- Vous voulez vous connecter au serveur de votre banque...
- Vous voulez envoyer un mail secret a une personne que vous ne connaissez pas ?

- Problème de transmission des clefs ?
- Problème du nombre de clefs pour un echange a n participants il faut n*(n+1)/2 clefs.

II. Cryptographie asymétrique

Idée de base : Une clef pour chiffrer , et une clef pour déchiffrer.

Fonctions de chiffrement / Déchiffrement : Des maths.

les deux clefs sont liées mathématiquement.
- Une clef privée (conservée précieusement par son propriétaire).
- Une clef publique (à diffuser partout).

II. Cryptographie asymétrique

Applications :

- Vous chiffrez vos compte rendus de TP avec ma clef publique.
=> je suis le seul a pouvoir déchiffrer (confidentialité).
(mais on peut faire un fake de l'un d'entre vous)

- Vous chiffrez vos compte rendus de TP avec votre clef privée
=> Vous etes le seul a pouvoir les avoir ecrits (authentification).
(mais tout le monde peut les lire).

Un algorithme de chiffrement

RSA.

III. Cryptographie hybride

Mélange des deux :

Exemple simple : Connexion a un site web dont vous connaissez la clef publique.

- Vous lui envoyez une clef secrète, chiffrée avec sa clef publique.
- Vous communiquez avec cette clef secrète.

Ça commence a ressembler à quelque chose...

Connaissez vous la clef publique de tous les sites ?
Comment récupérer les clefs publiques ? (Man in the Middle).

Signatures numériques

Comment signer un document ?