Cryptographie, clés et certificat

EGSI – 3ème année

CHARGE(E) DE PROJETS EN SYSTEMES INFORMATIQUES APPLIQUES - Option Sécurité Informatique

2022

Table des matières

Objectif du cours

- Enseignements théoriques et mises en pratique via un projet de programmation d'algorithmes de chiffrement de documents.
- Comprendre les mécanismes de la cryptographie
- Connaissances mathématiques et algorithmiques nécessaires, pratique de la programmation au service de la cryptographie.
- A l'issue du cours, être capable d'utiliser les outils de cryptographie

1. Introduction générale

1. Introduction générale

- Communication sécurisée :
  - Trafic Web : HTTPS
  - Trafic sans fil : 802.11i WPA2, GSM, Bluetooth
- Fichiers chiffrés : EFS, Truecrypt
- Protection de contenu : (DVD, Bluray) : CSS (content scrambling system), AACS
- Authentification utilisateur

1.1 Communication sécurisée

- Nos amis Alice et Bob
- Alice essaie essentiellement de communiquer en toute sécurité avec Bob
- Alice est sur l'ordinateur et Bob sur le serveur Web
- Le protocole utilisé est appelé HTTPS (SSL ou TLS en fait)
- Les buts de ces protocoles sont essentiellement de s'assurer
  - que les données circulent sur le réseau,
  - qu'un attaquant ne peut pas espionner des données et
  - qu'il ne peut pas les modifier tant qu'elles sont sur le réseau.

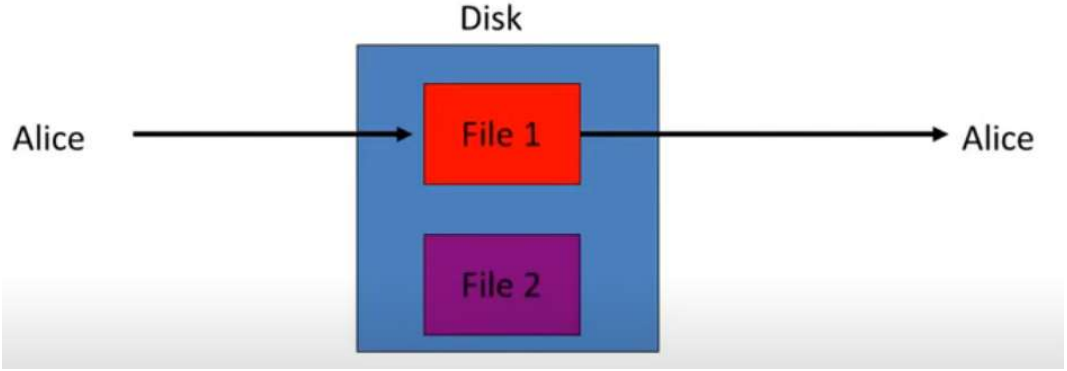
1.2 Secure Sockets Layer / Transport Layer Secure

Le protocole pour sécuriser le trafic Web est appelé TLS . Il se compose en 2 parties :

1. Handshake (ou poignée de main) : Alice et Bob parlent l'un avec l'autre, et à la fin du handshake , une clé secrète apparait entre eux. Les 2 connaissent la clé secrète, mais un attaquant qui observe la conversation n'a aucune idée de ce qu'est cette clé K. La façon dont on établit le handshake utilise la cryptographie à clé publique.
2. Maintenant que Alice et Bob ont partagé cette clé, nous pouvons utilisé cette clé pour communiquer en toute sécurité en chiffrant correctement les données entre eux.

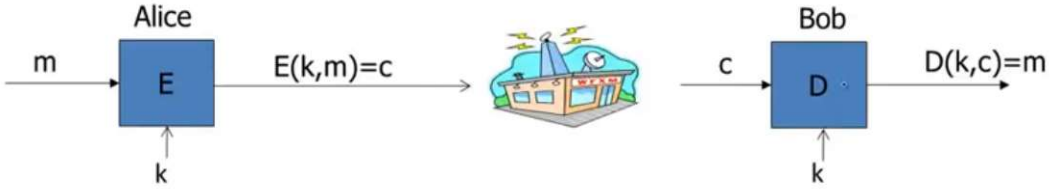
1.3 Fichiers protégés

- Une application de la cryptographie de protéger les fichiers sur les supports.



- Un fichier qui est chiffré même si le disque est volé, un attaquant ne peut pas réellement lire le contenu du fichier
- Si un attaquant essaie de modifier les données du fichier tout en étant sur le disque quand Alice essaie de déchiffrer ce fichier, ce sera détecté et elle va ignorer le contenu du fichier
- confidentialité et intégrité des fichiers stockés sur les supports

1.4 Chiffrement symétrique



- Les algorithmes E et D, les algorithmes réels sont connus du grand public, l'attaquant sait exactement comment ils fonctionnent.
  - **NE JAMAIS UTILISER D'ALGORITHME PROPRIETAIRE**
- 2 Cas d'usage du chiffrement symétrique:
  - Chaque clé n'est utilisée que pour chiffrer un seul message. C'est ce que l'on appelle les clés à usage unique. C'est par exemple quand on chiffre des emails. On va utiliser une clé différente pour chaque email.
  - La même clé est utilisée pour chiffrer plusieurs messages. C'est ce que l'on appelle les clés à usage multiples

2. Qu’est-ce que la cryptographie ?

2.1 Définition

- C’est la discipline qui traite de la **transmission confidentielle** de données.
- Remonte à l’antiquité et a connu un bouleversement profond à la fin du 20ème siècle.
- Deux types de cryptographie :
  - La cryptographie à clé secrète ou cryptographie symétrique. C’est la plus ancienne.
  - La cryptographie à clé publique ou cryptographie asymétrique. C’est la plus récente.
- Le chiffrement symétrique est beaucoup plus rapide
- Mais nécessite le partage au préalable d’une clé secrète
- La cryptographie se compose essentiellement de 2 parties :
  - L’établissement de la clé secrète
  - Comment communiquer en toute sécurité, une fois qu’on a partagé la clé secrète

2.2. D’autres exemples

- 2.2.1. La signature numérique
  - Une signature numérique est essentiellement analogue à une signature physique
  - Difficile à copier d’un document à un autre
  - Les signatures sont essentiellement fonction du contenu à signer

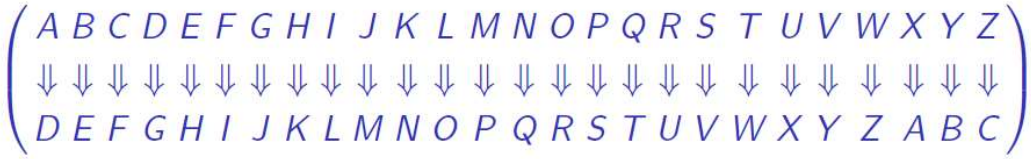
- 2.2.2. La communication anonyme
  - Il existe une méthode qui s’appelle Mix network qui permet à Alice de communiquer sur Internet avec Bob par une suite de proxys telle qu’à la fin de la communication, Bob n’a aucune idée à qui il vient de parler,
  - Les messages sont chiffrés et déchiffrés de manière appropriée afin que Bob ne sache pas à qui il a parlé, et les proxys eux-mêmes ne savent pas que Alice parle à Bob, ou de manière plus générale qui parle à qui.
  - Ce canal de communication anonyme est bidirectionnel : Bob, même s’il ne sait pas à qui il parle, il peut répondre à Alice, et Alice reçoit ses messages

3. Histoire rapide de la cryptographie

3.1. Quelques exemples d’algorithmes symétriques

- Le chiffrement de César

Le chiffre de César utilisé par Jules César dans ses correspondances :



Suétone rapporte que Jules César utilisait systématiquement le décalage de trois lettres ci-dessus, donc la même clé.

- Le chiffrement de Vigenère

Utilise le chiffre de César sauf que le décalage de chaque lettre du texte en clair est dépendant de la position celle-ci dans le texte. Ce décalage est calculé à l’aide d’une clé secrète. Cet algorithme, contrairement au précédent, résiste à l’analyse par fréquences mais a été cassé par Kasiski en 1863.

3.1. Quelques exemples d'algorithmes symétriques

Le chiffrement de Vernam

Le chiffre de Vernam (1926) est un chiffre de Vigenère où la clé secrète, de même longueur que le message à chiffrer, est choisie aléatoirement et n'est utilisée qu'une fois, théoriquement incassable mais sa mise en œuvre est difficile en pratique.

Autres

Une liste non exhaustive d'algorithme de chiffrements symétriques datant de la période « moderne » : DES (n'est plus utilisé), 3DES (variante du précédent), AES (le standard actuel en trois déclinaisons : 128, 192 et 256 bits), RC4, RC5 et d'autres encore.

3.2. Algorithmes asymétriques

- Ces algorithmes ont besoin de deux clés :
  - Une clé publique qui sert au chiffrement ou parfois aussi à la vérification de signature,
  - Une clé privée qui sert au déchiffrement ou parfois aussi à la signature.
- Le plus connu d'entre eux : RSA (Rivest, Shamir et Adleman en 1977). Il permet le chiffrement et la signature.
- Le protocole d'échanges de clés Diffie-Hellman (en 1976), protocole à l'origine de la cryptographie moderne,
- La cryptographie sur les courbes elliptiques
- L'algorithme de signature numérique DSA (Digital Signature Algorithm) proposé par le NIST

4. Rappels mathématiques

4.1. Les ensembles d'entiers

- Théorème (division euclidienne dans $\mathbb{N}$)

Soient $a, b \in \mathbb{N}$ avec $b \neq 0$. Alors, il existe $q, r \in \mathbb{N}$ uniques, tels que : $a = bq + r$ avec $0 \leq r < b$.

- Corollaire (division euclidienne dans $\mathbb{Z}$)

Soient $a \in \mathbb{Z}$ et , $b \in \mathbb{N}$ avec $b \neq 0$. . Alors, il existe $q \in \mathbb{Z}$ et $r \in \mathbb{N}$ uniques, tels que : $a = bq + r$ avec $0 \leq r < b$.

- Propriété ($\mathbb{N}$ est bien ordonné)

Toute partie non vide de $\mathbb{N}$ a un plus petit élément. Cette propriété est d'ailleurs équivalente au principe de récurrence :

- Propriété (principe de récurrence)

Soit $P(n)$ une propriété de l'entier $n \in \mathbb{N}$. Supposons que l'on ait :

(1) $P(0)$ est vraie,

(2) $\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1)$

Alors $P(n)$ est vraie pout tout $n \in \mathbb{N}$.

4.2. Divisibilité

Définition

Soient $a, b \in \mathbb{Z}$. On dit que b divise a et on écrit $b|a$ s'il existe $q \in \mathbb{Z}$ tel que $a = bq$.

On dit également que b est un diviseur de a ou que a est un multiple de b.

Remarque

On voit que 0 ne divise que lui-même alors que tout entier $n \in \mathbb{Z}$ divise 0. Par ailleurs, les entiers 1 et -1 divisent tous les entiers.

Proposition

Pour tout $n \in \mathbb{Z}$, on a les propriétés suivantes :

(1) si n divise a et b, alors n divise a - b et a + b,

(2) si n divise a, alors n divise ka pour tout $k \in \mathbb{Z}$.

4.2. Divisibilité (PGCD)

Proposition (plus grand commun diviseur)

Soient $a, b \in \mathbb{Z}$ non tous deux nuls. Alors l'ensemble des diviseurs > 0 communs à a et b admet un plus grand élément appelé plus grand commun diviseur de a et b. On le note : $pgcd(a, b)$.

Exemples

- $pgcd(24,54) = 6$ ($54 = 9 \times 6$ *et* $24 = 6 \times 4$),
- $pgcd(1, b) = 1$ *pour tout* $b \in \mathbb{Z}$
- $pgcd(0, b) = b$ *pour tout* $b > 0$.

Définition

Soient $a, b \in \mathbb{Z}$. a et b sont dits ***premiers entre eux*** *si* $pgcd(a, b) = 1$.

4.3. Congruences

- Définition

Soit $n \in \mathbb{N}, n > 0$. *On dit que* $a, b \in \mathbb{Z}$ *sont congrus modulo* n *et on note* $a \equiv b \ (mod\ n)$ *si* n *divise* $a - b$

- Exemples
  - *Modulo 1, la notion de congruence n'a aucun intérêt car tous les nombres sont congrus.*
  - *Modulo 2, un nombre est congru à 0 ou 1 selon qu'il est pair ou impair.*

- Proposition

Soit $\mathrm{n} \in \mathbb{N}, \mathrm{n} > 0$. *Tout nombre* $\mathrm{a} \in \mathbb{Z}$ *est congru modulo n à un et un seul des nombres* $\{0, \ldots, \mathrm{n} - 1\}$

- Proposition (inverse modulo n pour la multiplication)

Soient $a, \mathrm{n} \in \mathbb{N}, \mathrm{a}, \mathrm{n} > 0$ *et premiers entre eux. Alors il existe* $\mathrm{b} > 0$ *tel que* $ab \equiv 1 \ (mod\ n)$