Mise en sécurité des communications

Fred Hémery

IUT Béthune
Département
Réseaux &
Télécommunications

TRC8 Sécurité Avancée — 07/08

Plan

Introduction

- Lors de communications avec le réseau Internet, la transmission utilise les réseaux publics.
- Les réseaux publics (sauf accord avec le prestataire de service) peuvent être écoutés par un tiers.
- Afin de permettre la transmission de données privées, il faut ajouter un mécanisme de chiffrement.
- Il existe différents outils qui mettent en place le chiffrement :
  - Le protocole SSH
  - Kerberos
  - IPSEC
  - Le protocole SSL

Que permet le chiffrement ?

Authentification Le chiffrement détermine de manière fiable l'identité de d'un utilisateur. Pour cela à chaque demande de connexion l'utilisateur devra fournir une preuve numérique de son identité.

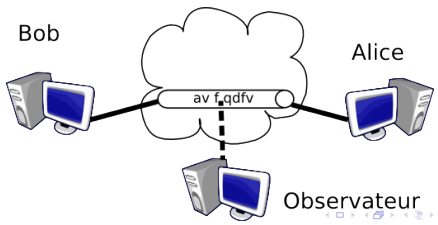
Confidentialité Un message reste confidentiel soit en limitant les autorisations d'accès ou encore en le rendant illisible.

Intégrité Elle garantit que les données passant sur le réseau ne seront pas modifiées.

Non répudiation Elle permet de garantir qu'une transaction a effectivement eu lieu.

Plantons le décor

- 3 composants
  1. Bob (partenaire de l'échange d'informations)
  2. Alice (partenaire de l'échange d'informations)
  3. Observateur
- Chiffrement : Transformation avant d'émettre sur le canal de communication
- Déchiffrement : Transformation après réception des données sur le canal.
- Décryptage : Tentative de transformation par l'observateur au cours de la transmission.



Modèle

Le chiffrement est un processus consistant à mélanger les données afin qu'elles ne puissent pas être lues par des personnes non autorisées.

- Données
  - κ : Clé
  - M : Message
  - C : Chiffré
  - F et F^{-1} : fonction de chiffrement et de déchiffrement
- Opération de chiffrement
  - $C = F(\kappa, M)$
- Opération de déchiffrement
  - $F^{-1}(\kappa, C) = F^{-1}(\kappa, F(\kappa, M)) = M$
- Propriétés
  - La détermination de la clé ne doit pas être possible
  - Transformation non linéaire

Modèle

- Les données originales sont appelées données en clair (*plaintext*), leur chiffrement donne des données chiffrées (*cyphertext*). Pour passer de l'un à l'autre on utilise un algo de chiffrement paramétré par une clé (secrète).
- L'algorithme de chiffrement est sûr si il est impossible à quiconque de lire les données chiffrées sans disposer de la clé.
- La **cryptanalyse** regroupe les techniques de déchiffrement des données sans utiliser la clé.
- Le **cryptographe** utilise les systèmes de chiffrement
- Le **cryptologue** conçoit les systèmes de chiffrement

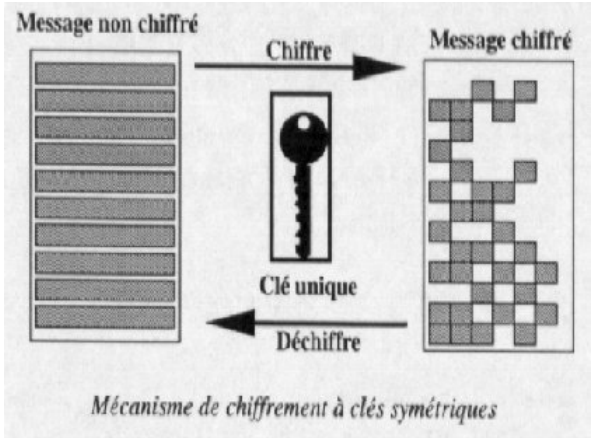
Techniques de chiffrement

Il existe deux catégories importantes de chiffrement :

- Le chiffrement à *clé secrète* (**symétrique**) qui utilise une seule clé pour chiffrer et déchiffrer les données.
  - Les algorithmes qui utilisent cette technique sont par exemple Blowfish, DES, IDEA, RC4, ...
- Le chiffrement à *clé publique* (**asymétrique**) qui utilise deux clés une pour le chiffrement et une pour le déchiffrement.
  - Les algorithmes qui utilisent cette technique sont par exemple RSA, ElGamal, Elliptic Curve, ...
  - Il existe une clé privée et une clé publique. La clé publique est utilisée par les correspondants pour transmettre des données chiffrées qui ne pourrons être lues que par le possesseur de la clé privée.

Plan

Cryptographie Symétrique



Mécanisme de chiffrement à clés symétriques

Cryptographie Symétrique

- Algorithme de César
  - Décale chaque caractère de k positions
  - k est la clé
  - exemple
    - ★ La chaîne de caractères : CECI EST UN EXEMPLE devient
    - ★ DFDJ FTU VO FYFNQMF
- Chiffrement par flux (stream cipher)
  - le flux provient d'un générateur pseudo aléatoire
  - XOR du flux et du texte en clair bit à bit
  - Ex : RC4
- chiffrement par bloc (bloc cipher)
  - Découpage du texte en clair en bloc de taille fixe et chiffrement de chaque bloc
  - Ex : DES, 3DES, AES
  - Un chaînage des blocs permet de crypter un bloc en fonction du bloc précédent.

Cryptographie Symétrique

Un algorithme est symétrique (à clé privée) si pour

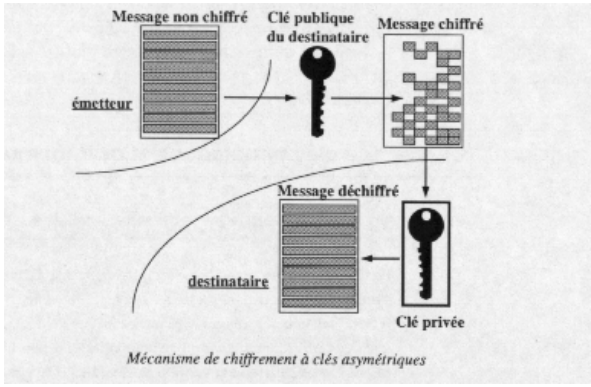
- $F^{-1}(\kappa_1, C) = F^{-1}(\kappa_2, F(\kappa_1, M)) = M$ alors $\kappa_1 = \kappa_2$

i.e. si la clé utilisée pour le cryptage est la même que celle utilisée pour le décryptage.

- Exemple DES
  - Fractionnement du texte en blocs de 64 bits avec une clé de 56bits
  - Permutation des blocs
  - Découpage des blocs en 2 sous-blocs
  - Permutation et substitution répétées 16 fois (ronde)
  - Fusion de 2 sous-blocs puis permutation initiale inverse
- 3DES
  - Basé sur DES
  - encrypté selon k_1, décrypté selon k_2, encrypté selon k_3
  - clé de 168bits
- AES
  - Algorithme de Rijndael
  - Clés de 128, 192, 256bits
  - Blocs de 128bits

Plan

Cryptographie Asymétrique



Mécanisme de chiffrement à clés asymétriques

Cryptographie Asymétrique

- Confidentialité
  - Un message chiffré avec la clé publique ne peut être déchiffré que par l'unique possesseur de la clé privée
- Signature
  - Un message chiffré avec la clé privée ne peut être déchiffré que par le possesseur de la clé publique
  - Identifie l'auteur du message (le possesseur de la clé privée)
  - La création d'une empreinte (Digest) signée permet de garantir l'intégrité du message.

Cryptographie Asymétrique

- Algorithmes de cryptographie pour la confidentialité
  - Diffie Helman (1976)
  - RSA : *Rivest Shamir Adelman* (1978)
- Algorithmes de cryptographie pour la signature
  - RSA
  - DSA *Digital Signature Algorithm*
  - Elliptic Curve Digital Signature Algorithm (ECDSA) est un algorithme de signature numérique et variante du standard DSA. Les avantages de ECDSA sur RSA sont des longueurs de clés plus courtes et des opérations de signature et de chiffrement plus rapide.

Diffie Helman

- Créer des clés symétriques sans avoir échangé un secret sur un canal sur.
- Algorithme
  - **A** et **B** s'envoient un nombre g et un nombre premier n
  - **A** choisit un grand nombre aléatoire x
  - **A** calcule $X = g^x(n)$ et l'envoie à **B**
  - **B** choisit un grand nombre aléatoire y
  - **B** calcule $Y = g^y(n)$ et l'envoie à **A**
- Ensuite **A** et **B**
  - **A** $\rightarrow k = Y^x(n)$
  - **B** $\rightarrow k' = X^y(n)$
- $k = k' = g^{xy}(n) \rightarrow$ création d'un secret partagé avec en pratique x et y de l'ordre de 512 ou 1024 bits et n 2400 bits
- Cryptanalyse
  - Écoute de X, Y, g puis opération inverse
  - Homme du milieu qui peut intercepter les échanges sans se faire remarquer.

RSA

- La clé de codage est publique (vous la fournissez à vos correspondants pour qu'ils cryptent les messages à votre destination), la clé de décodage privée (il n'y a que vous qui êtes en mesure de décoder les messages qui vous sont envoyés).
  - Choisir 2 nombres premiers, p et q,
  - chacun plus grand que 10100
  - Calculer $n = p \times q$ et $z = (p-1) \times (q-1)$
  - Choisir d premier avec z.
  - Clé publique : (e, n)
  - Clé privée : (d, n)
- Chiffrement
  - $C = M^e modulo(n)$
- Déchiffrement
  - $M = C^d modulo(n)$ car $C^d = (M^e)^d = M^{ed} = Mmodulo(n)$
- La force de RSA est qu'il est très difficile (dans un temps raisonnable) de faire une décomposition en facteurs premiers (on ne peut pas retrouver p et q en un temps raisonnable, donc z donc d à partir de n et e).

RSA (Exemple)

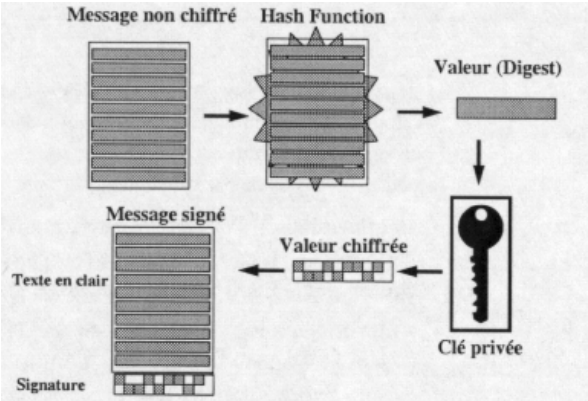
- On choisit : $p = 3$ et $q = 11 \rightarrow n = 33$ et $z = 20$
- On choisit $d = 7$ (premier avec z)
- On calcule : e tel que $7 \times e = 1(mod 20) \rightarrow e = 3$
- Un texte T en clair $\rightarrow C$ message crypté obtenu en calculant $C = T^3(mod 33)$
- Le récepteur déchiffre C en calculant
- $T = C^7(mod 33)$ T doit être plus petit que 33 : on peut mettre un caractère (lettre) dans chaque bloc du message T

car	valeur	p^3	$p^3(mod 33)$	C^7	$C^7(mod 33)$	car
S	19	6 859	28	13 492 928 512	19	S
U	21	9 261	21	1 801 088 541	21	U
Z	26	17 576	20	1 280 000 000	26	Z
A	01	1	1	1	01	A
N	14	2 744	5	78 125	14	N
N	14	2 744	5	78 125	14	N
E	05	125	26	8 031 810 176	05	E

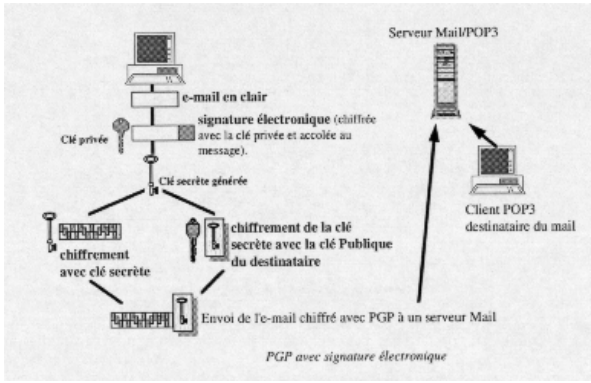
Signature : le principe

- Les fonctions de hachage
  - Une fonction de hachage permet de faire correspondre à un grand volume d'informations un volume réduit. Par exemple de 50000 octets on arrive à une correspondance de 128 octets.
  - La propriété importante d'une fonction de hachage est de garantir que si une petite modification est faite dans le volume d'informations alors la correspondance sera très différente.
  - Les fonctions de hachage sont par exemple **MD5** (*Message Digest #5*) , **SHA-1** (*Secure Hash Algorithm*)
  - Elles sont utilisées pour faire du contrôle d'intégrité, mais aussi pour le contrôle d'erreur
  - Il est très difficile de remonter de l'empreinte au texte original
  - Il est très difficile de produire la même empreinte avec deux documents différents à la base.

Signature éléctronique : un exemple d'utilisation



La méssagerie éléctronique : autre exemple d'utilisation



Plan

- Cryptographie Asymétrique
  - Avantages
    - ★ Utilisation de la signature
    - ★ Un couple de clès (privée/publique) suffisant
  - Inconvénients
    - ★ Calculs lents
    - ★ Validation de la clé publique
- Cryptographie Symétrique
  - Avantages
    - ★ Plus rapide
    - ★ Adapter au flux de données
  - Inconvénients
    - ★ Une clé pour chacun des correspondants
    - ★ n personnes $\rightarrow (n-1)$ clés. Comment faire la distribution ?

Solution : Combiner les deux !

1. Initiation d'une connexion avec du cryptage asymétrique (authentification)
2. négotiations de clés symétriques (clés de session)
3. Communication en utilisant les clés de session

- Utilisation de ce principe dans le protocole SSL et VPN

Les certificats

- La falsification des clés est une faiblesse majeure de la sécurité des crypto-systèmes à clé publique.
- Par exemple : supposons que Chloé veuille surveiller les messages que Alice envoie à Bob. Elle utilise une attaque de l'homme du milieu :
  - Chloé crée une nouvelle paire de clés ;
  - Elle remplace la copie d'Alice de la clé publique de Bob par la nouvelle clé publique ;
  - Elle intercepte les messages que Alice envoie à Bob. Pour chaque message, elle le déchiffre (avec la clé privée) et la chiffre en utilisant la clé publique de Bob
  - Tous les messages envoyés par Alice à Bob peuvent maintenant être lus par Chloé.

Les certificats

- Il faut s'assurer que la clé publique que l'on utilise appartient bien à l'utilisateur avec lequel on veut communiquer.
- On utilise pour cela un tiers de confiance qui délivre des clés publiques dans un certificat.
- Le certificat est établi par un organisme de confiance à la demande d'un utilisateur et contient :
  - La clé publique de l'utilisateur
  - Son nom
  - L'organisme de certification
  - Un numéro de série
  - Etc ...
  - Le certificat est donné à l'utilisateur sous forme chiffré avec la clé privée de l'organisme de certification

Les certificats

- Transmission normalisée d'un clé publique
- Certifiée par une CA (Certificate Authentication)
- Certificats X509
  - Versions
    - 1(1988), 2(1993), 3(1996)
    - Norme décrivant le certificat en l'ASN.1
    - Utilisés dans : SMIME, IPsec, SSL, horodatage, . . .
  - Contenu
    - version,
    - serial number (Numéro de série attribué par le CA)
    - issuer (identité du CA)
    - validity (la date d'activation et d'expiration)
    - subject (à qui appartient ce certificat)
    - subject public key information (la clé publique et des paramètres éventuels)
    - signature (le CA signe le certificat)
    - extensions (uniquement dans la V3) indique pour quel usage il doit être utilisé.

Les certificats

```
Certificate:
    Data:
        Version: 1 (0x0)
        Serial Number: 7829 (0x1e95)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=ZA, ST=Western Cape, L=Cape Town, O=Thawte Consulting cc,
                OU=Certification Services Division,
                CN=Thawte Server CA/Email=server-certs@thawte.com
        Validity
            Not Before: Jul  9 16:04:02 1998 GMT
            Not After : Jul  9 16:04:02 1999 GMT
        Subject: C=US, ST=Maryland, L=Pasadena, O=Brent Baccala,
                 OU=FreeSoft, CN=www.freesoft.org/Email=baccala@freesoft.org
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:b4:31:98:0a:c4:bc:62:c1:88:aa:dc:b0:c8:bb:
                    33:35:19:d5:0c:64:b9:3d:41:b2:96:fc:f3:31:e1:
                    66:36:d0:8e:56:12:44:ba:75:eb:e8:1c:9c:5b:66:
                    70:33:52:14:c9:ec:4f:91:51:70:39:de:53:85:17:
                    16:94:6e:ee:f4:d5:6f:d5:ca:b3:47:5e:1b:0c:7b:
                    c5:cc:2b:6b:c1:90:c3:16:31:0d:bf:7a:c7:47:77:
                    8f:a0:21:c7:4c:d0:16:65:00:c1:0f:d7:b8:80:e3:
                    d2:75:6b:c1:ea:9e:5c:5c:ea:7d:c1:a1:10:bc:b8:
                    e8:35:1c:9e:27:52:7e:41:8f
                Exponent: 65537 (0x10001)
    Signature Algorithm: md5WithRSAEncryption
        93:5f:8f:5f:c5:af:bf:0a:ab:a5:6d:fb:24:5f:b6:59:5d:9d:
        92:2e:4a:1b:8b:ac:7d:99:17:5d:cd:19:f6:ad:ef:63:2f:92:
        ab:2f:4b:cf:0a:13:90:ee:2c:0e:43:03:be:f6:ea:8e:9c:67:
        d0:a2:40:03:f7:ef:6a:15:09:79:a9:46:ed:b7:16:1b:41:72:
        0d:19:aa:ad:dd:9a:df:ab:97:50:65:f5:5e:85:a6:ef:19:d1:
```


Les certificats

- Les organismes de certification en France (exemples)
  - La Poste
  - la BNP ; le Crédit Lyonnais ; le Crédit Agricole ;
  - Click&trust ; Natexis ; le CCF ;
  - Certplus ; Certinomis,
  - Certimail (dont le service est un peu particulier) ;
  - Convergence ;
  - Certigreffe Certeurope
- Les organismes de certification doivent gérer le certificat dans le temps
- Nécessite de gérer des listes de certificats qui ne sont plus valides
- Une Interface de gestion de clés (IGC ou PKI) est l'ensemble des matériels, logiciels, personnes, règles nécessaires à une AC pour créer, gérer et distribuer des certificats X.509

Les certificats

- Certificat Revocation List (CRL)
  - Compromission d'un serveur, d'un PC, d'un collaborateur
  - Cessation d'un partenariat ⟶ Il faut révoquer le certificat (interdire son utilisation)
  - La CA maintient une liste de tous les certificats révoqués avant leur date d'expiration
  - Un noeud qui souhaite valider un certificat doit donc vérifier qu'il n'est pas dans cette liste
  - CRL :
    - date de révocation, numéro de série du certificat, prochaine CRL

Les certificats

- Chemin de certification
  - Une CA racine
    - Verisign, Thawte, . . .
  - Un arbre de CA
    - Délégation de la certification, dans un service pour une entreprise
  - Des certifications croisées entre certaines CA (Filiales)
  - Les feuilles
    - Utilisateurs finaux (pour le mail, . . .)
    - Serveurs (SSH, . . .)
- Chemin de validité (*Certificate Path Validation*)
  - Une cascade de certifications
  - Un noeud doit :
    - Vérifier chaque certification
    - Récupérer les listes de révocations éventuelles
  - *Certificate Validation Protocol* : Proposition en cours pour calculer ce chemin en mode *offline*.

Les certificats

Un exemple : Le commerce électronique

- Marie est le client, Jean est le vendeur (Marie dispose du certificat de Jean)
  - Marie à partir de son poste
    - Elle signe électroniquement la commande avec sa clé privée
    - Elle fournit son certificat personnel crée par un organisme tiers
    - L'ensemble est chiffré avec la clé symétrique générée pour l'échange par Marie. La clé de l'échange est ajoutée chiffrée avec la clé publique de Jean
  - Jean à partir de son poste
    - Jean déchiffre la clé de l'échange avec sa clé privée
    - Il déchiffre le certificat de Marie et la commande signée électroniquement, il déchiffre la signature
    - Il compare l'empreinte reçue avec l'empreinte calculée

Les certificats

Un exemple : Le commerce électronique

- Marie est le client, Jean est le vendeur (Marie dispose du certificat de Jean)
  - Marie à partir de son poste
    - Elle signe électroniquement la commande avec sa clé privée — intégrité
    - Elle fournit son certificat personnel crée par un organisme tiers — authentifie
    - L'ensemble est chiffré avec la clé symétrique générée pour l'échange par Marie. La clé de l'échange est ajoutée chiffrée avec la clé publique de Jean
  - Jean à partir de son poste
    - Jean déchiffre la clé de l'échange avec sa clé privée
    - Il déchiffre le certificat de Marie et la commande signée électroniquement, il déchiffre la signature
    - Il compare l'empreinte reçue avec l'empreinte calculée

Les certificats

Un exemple : Le commerce électronique

- Marie est le client, Jean est le vendeur (Marie dispose du certificat de Jean)
  - Marie à partir de son poste
    - Elle signe électroniquement la commande avec sa clé privée — intégrité
    - Elle fournit son certificat personnel crée par un organisme tiers — authentifie
    - L'ensemble est chiffré avec la clé symétrique générée pour l'échange par Marie. La clé de l'échange est ajoutée chiffrée avec la clé publique de Jean — confidentialité
  - Jean à partir de son poste
    - Jean déchiffre la clé de l'échange avec sa clé privée
    - Il déchiffre le certificat de Marie et la commande signée électroniquement, il déchiffre la signature
    - Il compare l'empreinte reçue avec l'empreinte calculée

Les certificats

Un exemple : Le commerce électronique

- Marie est le client, Jean est le vendeur (Marie dispose du certificat de Jean)
  - Marie à partir de son poste
    - Elle signe électroniquement la commande avec sa clé privée — intégrité
    - Elle fournit son certificat personnel crée par un organisme tiers — authentifie
    - L'ensemble est chiffré avec la clé symétrique générée pour l'échange par Marie. La clé de l'échange est ajoutée chiffrée avec la clé publique de Jean — confidentialité
  - Jean à partir de son poste
    - Jean déchiffre la clé de l'échange avec sa clé privée — authentifie
    - Il déchiffre le certificat de Marie et la commande signée électroniquement, il déchiffre la signature
    - Il compare l'empreinte reçue avec l'empreinte calculée

Les certificats

Un exemple : Le commerce électronique

- Marie est le client, Jean est le vendeur (Marie dispose du certificat de Jean)
  - Marie à partir de son poste
    - Elle signe électroniquement la commande avec sa clé privée — intégrité
    - Elle fournit son certificat personnel crée par un organisme tiers — authentifie
    - L'ensemble est chiffré avec la clé symétrique générée pour l'échange par Marie. La clé de l'échange est ajoutée chiffrée avec la clé publique de Jean — confidentialité
  - Jean à partir de son poste
    - Jean déchiffre la clé de l'échange avec sa clé privée — authentifie
    - Il déchiffre le certificat de Marie et la commande signée électroniquement, il déchiffre la signature
    - Il compare l'empreinte reçue avec l'empreinte calculée — intégrité

Plan

Gnu Privacy Guard

- GPG est un outil qui permet de mettre en place des communications sécurisées.
- Il permet notamment :
  - La création, l'échange et la vérification des paires de clés ;
  - Le chiffrement et le déchiffrement de documents
  - L'authentification avec des signatures électroniques

Gnu Privacy Guard

- Générer une nouvelle paire de clés : `gpg -gen-key`
- Lister les clés disponibles : `gpg -list-keys`
- Exporter une clé publique : `gpg -a -o fichier.gpg -export nomCle`
- Importer une clé publique : `gpg -i fichier.gpg`
- Chiffrer un document :
  - `gpg -a -o doc.gpg -encrypt -recipient ClePubliqueDestinataire doc`
- Déchiffrer un document :
  - `gpg -o doc -decrypt doc.gpg`
- Générer une signature : `gpg -a -o doc.sig -sign doc` (Le fichier contient le document d'origine et la signature éléctronique)
- Générer une signature avec document en clair : `gpg -a -o doc.sig -clearsign doc`
- Vérifier une signature : `gpg -verify doc.sig`

Plan

OpenSSL

- OpenSSL est un outil très complet (bibliothèque), il permet de créer et gérer des couples de clés(privée,publique), des AC, des CRL.
- Il supporte de nombreux algorithmes de chiffrement et d'empreinte de message.
- on utilise le programme `openssl` pour accéder aux fonctionnalités de la bibliothèque.
- `$ openssl <commande> [options pour cette commande]`
- par exemple, la commande `ca` gère les autorités de certification, la commande `md5` regroupe les fonctionnalités relatives au hashage *MD5*.

OpenSSL

- Création d'une IGC simple
  - Une autorité de certification
  - Un certificat pour une application (Apache)
  - Un certificat pour un utilisateur
  - Une CRL
- Création d'un certificat pour IGC
  - `openssl req -x509 -newkey rsa :1024 -days 3650 -keyout cakey.pem -out cacert.pem`
  - L'AC est maintenant configurée, on peut commencer à signer des demandes de certificat.
- Pour faire une demande de certificat, on crée un couple de clès à faire signer
  - `openssl req -newkey rsa :1024 -keyout cle-privee.key -out cle-publique.req`
  - Pour signer la demande de certificat
  - `openssl ca -in cle-publique.req -out certificat.pem`

OpenSSL

- Création d'un certificat pour "Robert Duchmol"
  - `openssl req -newkey rsa :1024 -keyout client.key -out client.req`
  - il faut que l'AC signe la demande de certificat
  - `openssl ca -in client.req -out client.pem`
  - Pour pouvoir importer le couple de clés de l'utilisateur dans un navigateur web, il faut que celui soit au format **PKCS#12**
  - `openssl pkcs12 -export -in client.pem -inkey client.key -out r_duchmol.p12 -name "Robert Duchmol"`
  -
- Générer des listes de révocation (CRL)
  - Robert Duchmol perd la clé privée de son certificat ou se fait voler son fichier PKCS#12, l'AC doit révoquer son certificat
  - `openssl ca -revoke /etc/ssl/newcerts/02.pem` (`02.pem` est le certificat de Robert Duchmol)
  - Générer la CRL pour le serveur
  - `openssl ca -gencrl -out /etc/ssl/crl.pem`