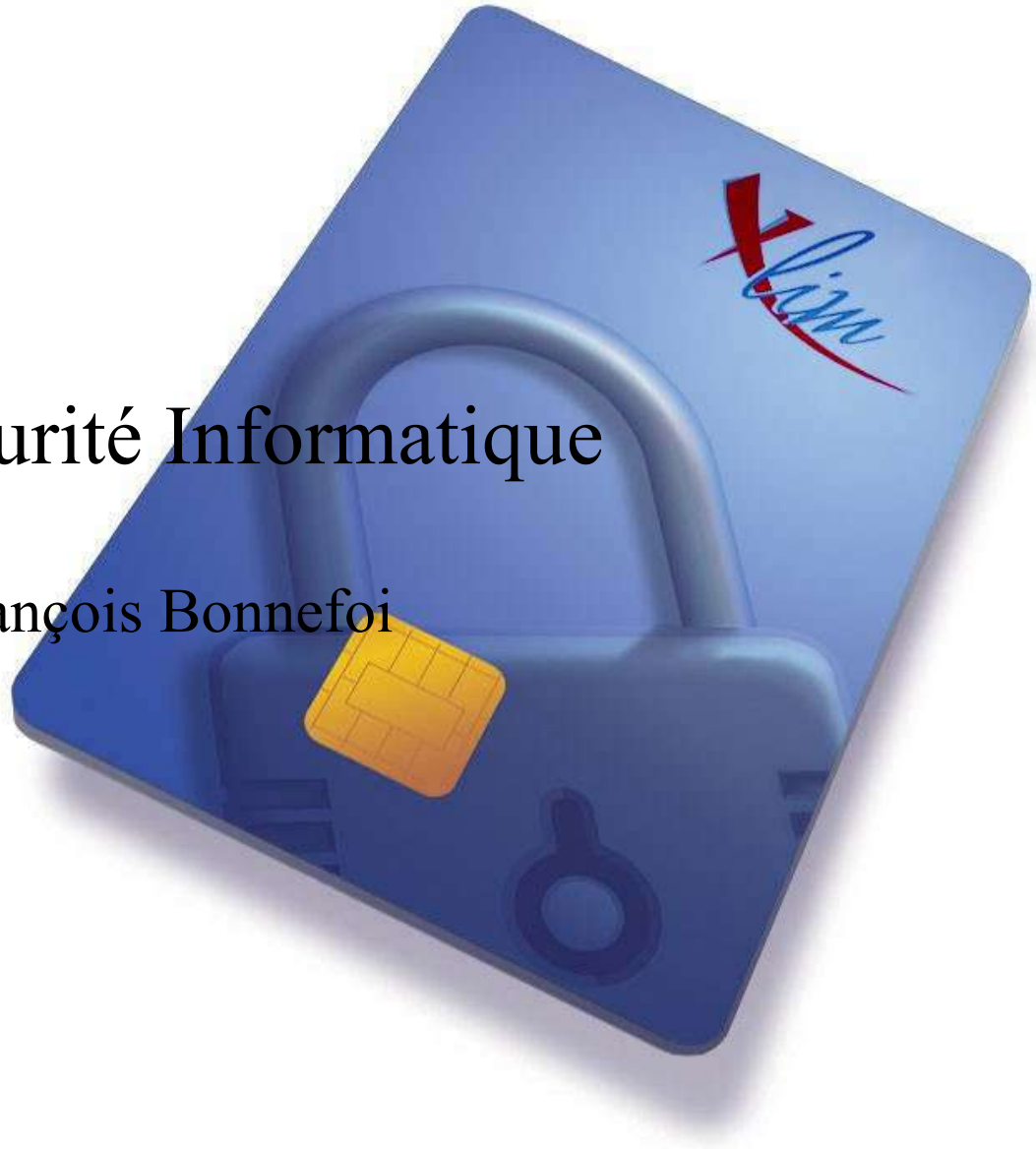
Cours de Sécurité Informatique

Pierre-François Bonnefoi



Quels sont les risques ?

Evaluation des risques liées à l'utilisation de l'informatique

Il importe de mesurer ces risques :

- en fonction de la probabilité ou de la fréquence de leurs survenances ;
- en mesurant leurs effets possibles.

Ces effets peuvent avoir des conséquences **négligeables** ou **catastrophiques :**

- le traitement informatique en cours échoue : il suffit de le relancer, éventuellement par une autre méthode si on craint que la cause ne réapparaisse ;
- l'incident est bloquant et on doit procéder à une réparation ou une correction avant de poursuivre le travail entrepris.

Mais ces mêmes incidents peuvent avoir des conséquences beaucoup plus fâcheuses :

- **données irrémédiablement perdues** ou **altérées**, ce qui les rend inexploitables ;
- **données** ou **traitements durablement indisponibles**, pouvant entraîner l'arrêt d'une production ou d'un service ;
- **divulgation d'informations confidentielles** ou **erronées** pouvant profiter à des sociétés concurrentes ou nuire à l'image de l'entreprise ;
- déclenchement d'actions pouvant provoquer des **accidents physiques** ou induire des **drames humains**.

Les risques humains

Ce sont les plus importants, même s'ils sont le plus souvent ignorés ou minimisés.
Ils concernent les utilisateurs mais également les informaticiens eux-mêmes.

- la **maladresse** : commettre des erreurs : exécuter un traitement non souhaité, effacer involontairement des données ou des programmes, etc.

- **l'inconscience** et **l'ignorance** : introduire des programmes malveillants sans le savoir (par exemple lors de la réception de courrier).
  De nombreux utilisateurs d'outils informatiques sont encore inconscients ou ignorants des risques qu'ils font courir aux systèmes qu'ils utilisent.
  Réaliser des manipulations inconsidérées (autant avec des logiciels qu'avec du matériel)

- la **malveillance** : impossible d'ignorer les différents problèmes de virus et de vers ces dernières années (beaucoup de couverture médiatique).
  Certains utilisateurs peuvent volontairement mettre en péril le système d'information, en y introduisant en connaissance de cause des virus (en connectant par exemple un ordinateur portable sur un réseau d'entreprise), ou en introduisant volontairement de mauvaises informations dans une base de données.
  Il est facile pour un informaticien d'ajouter délibérément des fonctions cachées lui permettant, directement ou avec l'aide de complices, de détourner à son profit de l'information ou de l'argent.

  On parle alors de la « cyber-criminalité ».

Les risques humains

- **l'ingénierie sociale** (*social engineering*) est une méthode pour obtenir d'une personne des informations confidentielles, que l'on n'est pas normalement autorisé à obtenir, en vue de les exploiter à d'autres fins (publicitaires par exemple).

  Elle consiste à :
  - se faire passer pour quelqu'un que l'on est pas (en général un administrateur)
  - demander des informations personnelles (nom de connexion, mot de passe, données confidentielles, etc.) en inventant un quelconque prétexte (problème dans le réseau, modification de celui-ci, heure tardive, etc.).
  Elle peut se faire soit au moyen d'une simple communication téléphonique, soit par mail, soit en se déplaçant directement sur place.

- **l'espionnage** : surtout industriel, emploie les même moyens, ainsi que bien d'autres, pour obtenir des informations sur des activités concurrentes, procédés de fabrication, projets en cours, futurs produits, politique de prix, clients et prospects, etc.

  Des formes à la limite de la légalité correspondent à « **l'intelligence économique** ».

Les risques matériels

Ils sont liés aux défauts et pannes **inévitables** que connaissent tous les systèmes matériels et logiciels. Ces incidents sont plus ou moins fréquents selon le soin apporté lors de la fabrication et l'application de procédures de tests effectuées avant que les ordinateurs et les programmes ne soient mis en service. Certaines de ces pannes ont des causes indirectes, voire très indirectes, donc **difficiles à prévoir**.

- **Incidents liés** au **matériel** : la plupart des composants électroniques, produits en grandes séries, peuvent comporter des défauts.
  Ils finissent un jour ou l'autre par tomber en panne.
  Certaines de ces pannes sont assez difficiles à déceler car **intermittentes** ou **rares**.
  Parfois, elles relèvent d'une erreur de conception (*une des toutes premières générations du processeur Pentium d'Intel pouvait produire, dans certaines circonstances, des erreurs de calcul*) ;

- **Incidents liés** au **logiciel** : mes plus fréquents ;
  Les systèmes d'exploitation et les programmes sont de plus en plus complexes car ils font de plus en plus de choses. Ils nécessitent l'effort conjoint de dizaines, de centaines, voire de milliers de programmeurs. Ces programmeurs peuvent faire des erreurs de manière individuellement ou collective que les meilleures méthodes de travail et les meilleurs outils de contrôle ou de test ne peuvent pas éliminer en totalité.

- **Incidents liés** à **l'environnement** : les machines électroniques et les réseaux de communication sont sensibles aux variations de température ou d'humidité (tout particulièrement en cas d'incendie ou d'inondation) ainsi qu'aux champs électriques et magnétiques.
  Il es tpossible qu'un ordinateur tombe en panne de manière définitive ou intermittente à cause de conditions climatiques inhabituelles ou par l'influence d'installations électriques notamment industrielles (et parfois celle des ordinateurs eux-mêmes !).

Les précautions à prendre

Dans le cas des riques matériels il est possible de se prémunir :

- **redondance des matériels** : la probabilité ou la fréquence de pannes d'un équipement est représentée par un nombre très faible (compris entre 0 et 1, exprimé sous la forme 10^-n).
  En doublant ou en triplant (ou plus) un équipement, on divise le risque total par la probabilité de pannes simultanées.
  Le résultat est donc un nombre **beaucoup plus faible** et la fiabilité est plus grande.

- **dispersion des sites** : un accident (incendie, tempête, tremblement de terre, attentat, etc.) a très peu de chance de se produire simultanément en plusieurs endroits distants.

- **procédures** de **contrôle indépendants** : ils permettent bien souvent de déceler les anomalies avant qu'elles ne produisent des effets dévastateurs.
  Il est possible de réaliser des **audits** de sécurité.

Sécurité et Sureté

On parle de :

- « **Sécurité** de fonctionnement » dans le cas de la protection des données et de la capacité de travail contre les actes de malveillance ;

- « **Sureté** de fonctionnement » dans le cas de la protection du système d'information contre les accidents

Les programmes malveillants

Un logiciel malveillant (malware en anglais) est un logiciel développé dans le but de nuire à un système informatique.

- le **virus** : programme se dupliquant automatiquement sur le même ordinateur.
  Il peut être transmis à un autre ordinateur par l'intermédiaire du courrier électronique ou par l'échange de données ;

- le **ver** (*worm*) : exploite les communications réseaux d'un ordinateur afin d'assurer sa reproduction sur d'autres ordinateurs ;

- le **cheval de Troie** (*trojan*) : programme à apparence légitime (voulue) qui exécute des routines nuisibles sans l'autorisation de l'utilisateur ;

- la **porte dérobée** (*backdoor*) : permet d'ouvrir d'un accès réseau frauduleux sur un système informatique. Il est ainsi possible d'exploiter à distance la machine ;

- le **logiciel espion** (*spyware*) : fait de la collecte d'informations personnelles sur l'ordinateur d'un utilisateur sans son autorisation. Ces informations sont ensuite transmises à un ordinateur tiers ;

- **l'enregistreur de frappe** (*keylogger*) : programme généralement invisible installé sur le poste d'un utilisateur et chargé d'enregistrer à son insu ses frappes clavier ;
  pour intercepter des mots de passe par exemple.

- **l'exploit** : programme permettant d'exploiter une faille de sécurité d'un logiciel ;

- le **rootkit** : ensemble de logiciels permettant généralement d'obtenir les droits d'administrateur sur une machine, d'installer une porte dérobée, de truquer les informations susceptibles de révéler la compromission, et d'effacer les traces laissées par l'opération dans les journaux système.

Les risques et menaces de la messagerie électronique

- le **pourriel** (*spam*) : un courrier électronique non sollicité, la plupart du temps de la publicité.
  Ils encombrent le réseau, et font perdre du temps à leurs destinataires ;

- **l'hameçonnage** (*phishing*) : un courrier électronique dont l'expéditeur se fait généralement passer pour un organisme financier et demandant au destinataire de fournir des informations confidentielles ;

- le **canular informatique** (*hoax*) : un courrier électronique incitant généralement le destinataire à retransmettre le message à ses contacts sous divers prétextes.
  Ils encombrent le réseau, et font perdre du temps à leurs destinataires.
  Dans certains cas, ils incitent l'utilisateur à effectuer des manipulations dangereuses sur son poste (suppression d'un fichier prétendument lié à un virus par exemple).

Les risques et menaces sur le réseau

- les **écoutes** (*sniffing*) : technique permettant de récupérer toutes les informations transitant sur un réseau (on utilise pour cela un logiciel sniffer).
  Elle est généralement utilisée pour récupérer les mots de passe des applications et pour identifier les machines qui communiquent sur le réseau.

- **l'usurpation d'identité** (*spoofing*) : technique consistant à prendre l'identité d'une autre personne ou d'une autre machine.
  Elle est généralement utilisée pour récupérer des informations sensibles, que l'on ne pourrait pas avoir autrement.

- le **déni de service** (*denial of service*) : technique visant à provoquer des interruptions deservice, et ainsi d'empêcher le bon fonctionnement d'un système.
  Il peut y avoir des tentatives d'extorsion de fond : menacer de stopper l'activité d'une entreprise.

Les usages d'Internet : les différents services

Le World Wide Web ou simplement Web

Utilisation de « **navigateur Web** », ou *butineur*, comme Firefox, Internet Explorer, Opera etc.

Le navigateur ou le nouveau « système d'exploitation » :

- La connaissance et l'accès au Web est souvent connue par l'intermédiaire du moteur de recherche !
- **Rivalités** pour le contrôle des moteurs de recherche : Google, Yahoo, Microsoft...
- Accès **partout** : dans des points d'accès libres, bornes internet à la Poste, CyberCafé ;
- Accès **sur tout** : téléphonie mobile, PDA (ordinateurs de poche), portables etc. ;
- Accès **pour tout** : utilisation pour passer des commandes, consulter et gérer son compte en banque, son compte mobile, envoyer du courrier et le consulter, communiquer de manière instantanée (chat) etc.
- **Substitution** à des applications métiers : la gestion des comptes bancaires des clients d'une banque, l'édition de document, le contrôle à distance des serveurs ;
- **Intranet** dans l'entreprise : solutions de travail collaboratif, portail d'entreprise, etc.

La messagerie

Instantanée : MSN, Yahoo, Caramail, IRC, Google Talk, Yahoo Messenger, etc.
Différée : le **courrier électronique** : il est équivalent au courrier papier et bénéficie du principe du « secret de la correspondance ».

La téléphonie IP

Convergence mobile, fixe, Internet : Unyk, NeufTalk, etc.
Solutions **propriétaires** : Skype
Solutions **semi-ouvertes** : la téléphonie SIP avec Free, N9uf, Orange, etc.

L'identité sur Internet

Comment est-on reconnu sur Internet pour l'utilisation d'un service ?

- On y accède par un ordinateur : l'identifiant de la machine ? Mais on peut changer d'ordinateur ;
- On fournit soit-même une information : un identifiant choisi, un *pseudo*, non déjà affecté à un autre utilisateur ;

Comment empêcher quelqu'un de prendre mon identité ? En cas de perte ?

- En plus de l'identifiant, on fournit un mot de passe que l'on conserve secret ;
- On fournit une adresse de messagerie vers laquelle le mot de passe ou un nouveau peut être envoyé en cas de perte : c'est l'adresse de messagerie et la possibilité d'en relever le courrier qui fournit la preuve de l'identité ;
- Dans le cas de la messagerie : on peut téléphoner à la « hotline » du FAI (Fournisseur d'Accès Internet), ou obtenir l'envoi d'un courrier papier. En définitive et dans le cas d'un service payant c'est la domiciliation bancaire qui sert de preuve.

Lors d'une communication, comment identifier les interlocuteurs ?

- Qui est à l'origine de l'appel dans le cas d'une messagerie instantanée ou différée ?
- Qui est derrière ce pseudo ?

Lors d'une commande passée sur Internet ?

- Quel est le serveur avec le lequel on communique ?
- Lorsque l'on fournit ses informations de paiement par carte bancaire, est-ce que ces informations serviront seulement à ce que je viens d'acheter et d'autoriser ?

Le phishing en action

Un courrier à l'apparence innocente arrive dans la boîte au lettre...
Le logiciel anti spam m'alerte d'un risque (mais il le fait pratiquement pour tous les courriers contenant un lien vers un site web...).

Sujet : {Spam?} Votre compte de Credit Mutuel
De : client-access@cmmd.creditmutuel.fr <client-access@cmmd.creditmutuel.fr>
Réponse à : client-access@cmmd.creditmutuel.fr
Date : 18/11/2006 09:54
Pour : undisclosed-recipients:;

Cher Client de CreditMutuel

En raison des erros multiple de login, votre accиs a CreditMutuel a йtй temporairement fermй.Protйger la sйcuritй de votre compte et du rйseau de CreditMutuel est notre inquiйtude primaire.

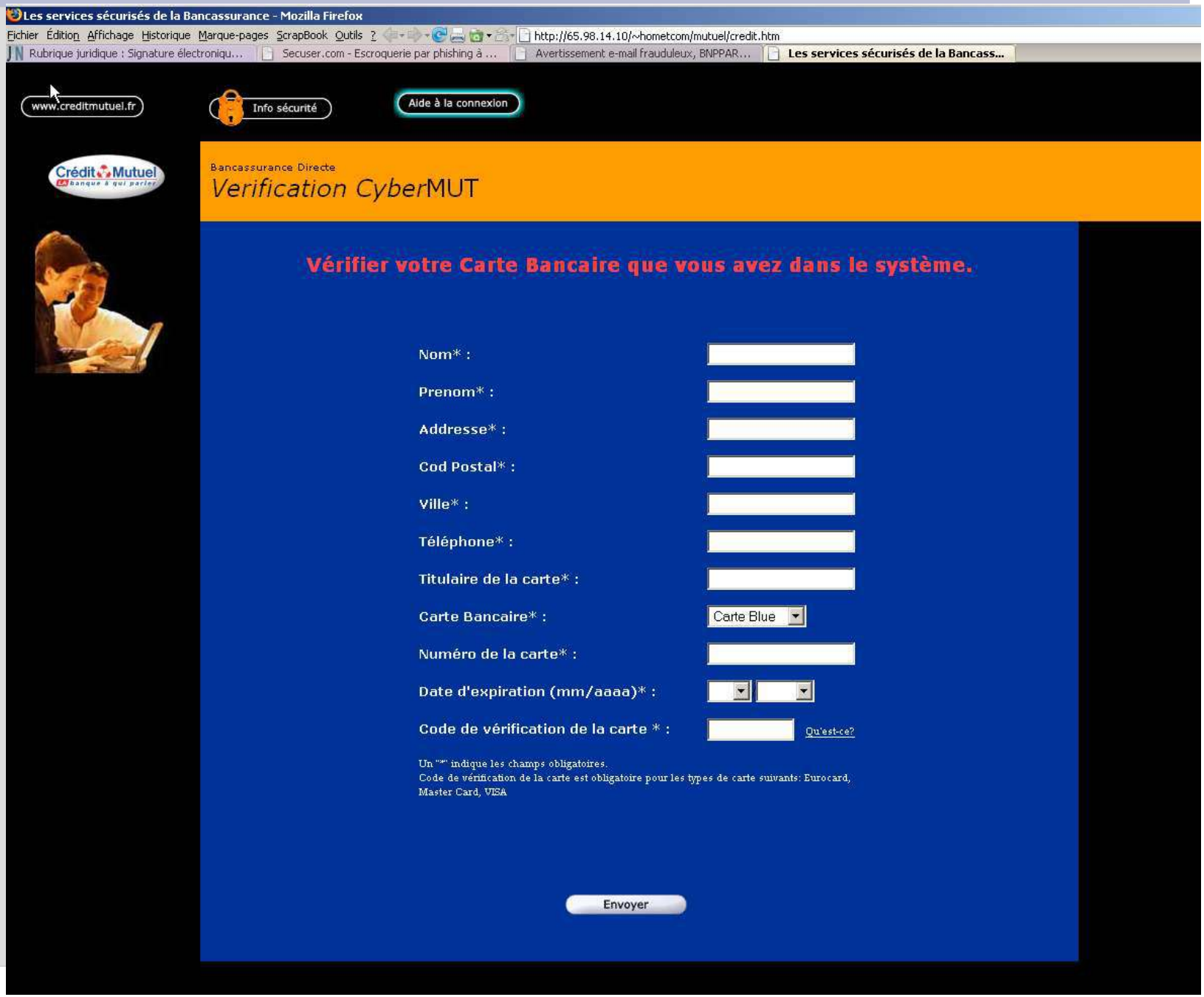
Donc, comme une mesure prйventive, nous avons limitй temporairement l'accиs aux caractйristiques sensibles de votre compte avec CreditMutuel.
Si vous кtes le titulaire lйgitime du compte, s'il vous plaot login a **MailScanner soupçonne le lien suivant d'être une tentative de fraude de la part de "www.webhost119.com"** http://www.creditmutuel.com/client-access/, comme nous essayons de vйrifier votre identitй.

Merci pour votre patience comme nous travaillons ensemble a protйger votre compte.

Copyright © 1999 E.I.D. (Groupe Crйdit Mutuel) - Juin 2001

Le phishing en action

En cliquant...



Les points de sécurité abordés dans le cours

La sécurité des identités
- Éviter l'usurpation d'identité ;
- Permettre l'authentification d'une identité.

Les solutions :
- Utiliser des algorithmes de chiffrement asymétrique ;
- Déployer une PKI (Public Key Infrastructure) ;
- Délivrer des certificats électroniques aux personnes ;
- Signer électroniquement les documents échangés.

La sécurité des échanges
- Éviter l'interception des données transmises (les mots de passe, etc.) ;
- Identifier les interlocuteurs.

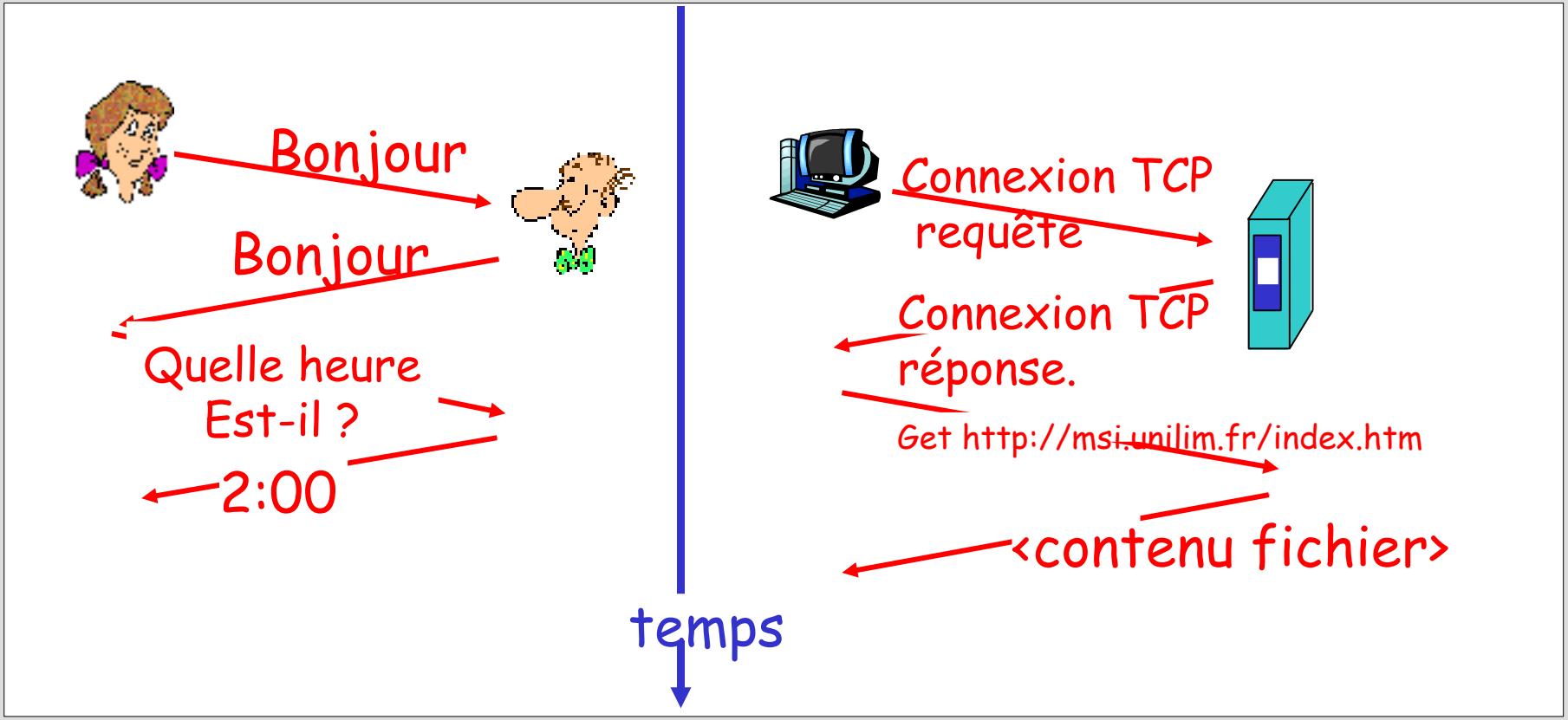
Les solutions :
- Utiliser des algorithmes de chiffrement symétrique et asymétrique ;
- Déployer une PKI ;
- Délivrer des certificats électroniques aux ordinateurs ;
- Authentifier les ordinateurs ;
- Rendre confidentiel les échanges : chiffrer leur contenu.

Les échanges sur un réseau ?
- Des protocoles utilisateur comme le HTTP ;
- Des échanges de messages sur les supports physiques de communication.

Qu'est-ce qu'un protocole

Un protocole humain et un protocole machine

« demander l'heure à quelqu'un » et « demander une ressource sur un serveur Web ».



Les protocoles définissent :

- le **format** ;
- l'**ordre** des messages émis et reçus entre les ordinateurs ;
- ainsi que les **réactions** à ces messages.

Le protocole HTTP support su Web

Définition de différents protocole

– HTTP “Hyper Text Transfer Protocol”

Ce protocole est le plus « en vue » sur Internet puisqu'il sert à la mise en œuvre du “Web” ou “World Wide Web” ou « Toile de taille mondiale ».

C'est un protocole simple permettant l'échange de données de différents types dont le plus célébre est le format “HTML Hyper Text Markup Language”.

Ce protocole a popularisé et est basé sur le concept d'“URL Uniform Resource Locator” qui permet de localiser simplement une resource sur Internet et d'indiquer également le moyen pour y accéder.

– ...

Des protocoles orientés « humains »

Ces protocoles ont en commun de se baser sur :

- l'utilisation de connexion TCP (flux d'octets, sans erreur, bidirectionnel, “full duplex”)
- l'échange de lignes de caractères sur 7bits (au moins pour le contrôle)
- l'utilisation de commandes et d'arguments lisible et interprétable par un humain
- Exemple : GET /index.html HTTP/1.0 cas de HTTP
  MAIL FROM: <toto@lablague.fr> cas de SMTP
- l'utilisation de contrôle d'erreur basé sur un nombre suivi d'un descriptif
  Exemple : 230 List of 2 articles follows cas de NNTP

Des protocoles étendus par encapsulation

Une fois un protocole défini pour organiser un échange, il ne rest plus qu'à transmettre les informations.

Ces informations sont codifiées dans un format qui peut être indépendant du protocole, c-à-d. que le protocole ne sait pas quelle nature de donnée il transmet et c'est au destinataire que revient la tâche de déterminer la nature du contenu et le moyen de le récupérer dans sa forme original.

Exemple : le transfert de courrier a été étendu pour transmettre des données binaires en codifiant ces données binaires dans un format texte à l'aide du système “MIME Multi-purpose Internet Mail Extension”.

Le concept d'URL “Uniform Resource Locator”

Localisation et accés à l'information

Le problème de l'accés aux données est un double problème, il faut indiquer :

- l'endroit où se trouve la resource;
- le moyen pour la récupérer avec éventuellement des autorisations d'accès.

Format universel

service :// adresse_machine [*:n° port*] / chemin_accés

La plupart des fois le nom du service correspond à celui du protocole

Exemple : http://www.sciences.unilim.fr
ftp://ftp.unilim.fr
mais également : news://news.unilim.fr

Peuvent être ajouté :

- une identité : ftp://toto@alphainfo.unilim.fr
- une identité et un mot de passe : ftp://toto:top_secret@ftp.unilim.fr
- un chemin d'accés à un répertoire ou à un fichier ou à un groupe :
  - ftp://ftp.unilim.fr/pub/mac
  - http://www.sciences.unilim.fr/index.htm
  - news://news.unilim.fr/fr.rec.*
- un numéro de port de connexion pour utiliser un numéro de port différent de celui par défaut du service (serveur utilisateur ne pouvant utilisé un port réservé par l'administrateur, serveur supplémentaire, port non filtré par un firewall…)

Dans le cas d'une localisation avec un chemin d'accès vers un répertoire ou un fichier, il est nécessaire de tenir compte des droits d'accès à ces ressources.

L'accès à un fichier peut être bloqué, ou le contenu d'un répertoire interdit en lecture.

Mais il peut être utile de modifier l'URL au niveau du chemin d'accès pour pouvoir accéder à une ressource qui aurait été déplacée (changement de répertoire ou de nom…).

Le courrier électronique – Format du courrier

Format du courrier

Un format très simple a été défini pour le courrier concernant l'identification de l'expéditeur et des destinataires, ainsi que le contenu du courrier (corps de la lettre).

Ces informations sont directement échangées au sein du protocole **SMTP**.

Pour la définition du courrier, une structure légère mais suffisante a été définie :

- pour les données, seul le format texte sur 7bits est toléré dans le SMTP classique
- le courrier contient un certain nombre de champs d'en-tête :
- To: pour les adresses des destinataires primaires sour forme d'entrée DNS
- From: personne qui a créé le message
- Subject: pour décrire le contenu du courrier
- Cc: (copie conforme) pour une liste de destinataires secondaires
- Received: ligne ajoutée par par chaque agent de transfert le long de la route empruntée par le courrier

  Cette information permet d'identifier les différents intermédiaires empruntés (tous les relais).
- Return-Path: adresse de retour ajoutée par l'agent de transfert de message final (définie à partir des informations données dans les champs received:)
- Reply-to: adresse DNS à utiliser pour répondre, souhaitée par l'expéditeur (peut être différente de celle indiquée par le “return-path:” en particulier à cause des alias.)
- Date: la date et heure d'envoi
- Message-Id: numéro unique permettant de référencer le message (lors d'échange successif de courrier)
- In Reply-to: donne la référence du message auquel on répond
- … des extensions peuvent être ajoutées en les préfixant pas X-

En général, seul les champs From: To: et Date: sont obligatoires.

Les champs d'en-tête sont séparés du corps du courrier par une ligne vide.

Le protocole SMTP

Exemple de transaction entre le client et le serveur suivant le protocole SMTP :

Action	*Client*	*Serveur*
Connexion du client au serveur		
Invite du serveur		220 serveur.unilim.fr
Présentation du client	HELO client.unilim.fr	
Salutation du serveur		250 Nice to meet you
Indication de l'expéditeur	MAIL FROM: <alice@msi.unilim.fr>	
Acceptation de l'expéditeur		250 Ok
Indication du destinataire	RCPT TO: <bob@ishtar.msi.unilim.fr>	
Acceptation du destinataire		250 Ok
Début du courrier	DATA	
Acceptation		354 Send the content of mail. Stop with \r\n.\r\n
Contenu du courrier	[...]	
Fin du contenu du courrier	.	
Validation du courrier		250 Ok
Fin de la connexion du client	QUIT	
Fin de la connexion du serveur		

Le courrier de phishing à analyser

```
Return-Path: <client-access@cmmd.creditmutuel.fr>
Received: from courriel.unilim.fr ([unix socket])
          by courriel.unilim.fr (Cyrus v2.2.12-Invoca-RPM-2.2.12-3.RHEL4.1) with LMTPA;
          Sat, 18 Nov 2006 10:05:18 +0100
X-Sieve: CMU Sieve 2.2
Received: from smtp.unilim.fr (mail.unilim.fr [164.81.1.45])
          by courriel.unilim.fr (Postfix) with ESMTP id 6F697340093
          for <bonnefoi@unilim.fr>; Sat, 18 Nov 2006 10:05:18 +0100 (CET)
Received: from n007.sc1.cp.net (smtpout1482.sc1.he.tucows.com [64.97.157.182])
          by smtp.unilim.fr (8.13.1/8.13.1) with ESMTP id kAI95GKr021369
          for <bonnefoi@unilim.fr>; Sat, 18 Nov 2006 10:05:16 +0100
Received: from User (64.34.102.43) by n007.sc1.cp.net (7.2.069.1) (authenticated as manimoch@savadaulamuie.com)
        id 455C77220008F2C7; Sat, 18 Nov 2006 08:54:37 +0000
Message-ID: <455C77220008F2C7@n007.sc1.cp.net> (added by postmaster@bouncemessage.net)
Reply-To: <client-access@cmmd.creditmutuel.fr>
From: "client-access@cmmd.creditmutuel.fr"<client-access@cmmd.creditmutuel.fr>
Subject: {Spam?} Votre compte de Credit Mutuel
Date: Sat, 18 Nov 2006 00:54:38 -0800

MIME-Version: 1.0
Content-Type: text/html;
          charset="Windows-1251"
Content-Transfer-Encoding: 7bit

<p> </p>
<p>Copyright © 1999 E.I.D. (Groupe Crédit Mutuel) - Juin 2001</p>
```

Qui est ce ?

Whols Result For savadaulamuie.com @ whois.melbourneit.com

Domain Name	**savadaulamuie.com**
Creation Date	**2006-06-24**
Registration Date	**2006-06-24**
Expiry Date	**2007-06-24**
Organisation Name	**Karen Blackmore**
Organisation Address	**43a Upper Northam Road**
	Southampton
	S030 4DY
	XX
	UNITED KINGDOM
Admin Name	**Karen Blackmore**
Admin Address	**43a Upper Northam Road**
	Southampton
	S030 4DY
	XX
	UNITED KINGDOM
Admin Email	**muieinnas@msn.com**
Admin Phone	**+1.**
Tech Name	**Name Tech**
Tech Address	**5190 Neil Road**
	Ste. 430
	Reno
	89502
	NV
	UNITED STATES
Tech Email	**nametech@netidentity.com**
Tech Phone	**+1.**
Name Server	**NS1.MAILBANK.COM**
	NS2.MAILBANK.COM

Qui est-ce ?

Domain Name: CP.NET
Registrar: EBRANDSECURE, LLC
Whois Server: whois.ebrandsecure.com
Referral URL: http://www.ebrandsecure.com
Name Server: NS1.CP.NET
Name Server: NS3.CP.NET
Name Server: NS2.CP.NET
Status: clientTransferProhibited
Status: clientUpdateProhibited
Status: clientDeleteProhibited
Updated Date: 29-mar-2006
Creation Date: 03-apr-1998
Expiration Date: 02-apr-2013

Le courrier de phishing à analyser

```
X-Priority: 1
X-MSMail-Priority: High
X-Mailer: Microsoft Outlook Express 6.00.2600.0000
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2600.0000
X-Univ-Limoges-Greylist: IP, sender and recipient auto-whitelisted, not delayed by milter-greylist-2.0.2 (smtp.unilim.fr [164.81.1.45]); Sat, 18
Nov 2006 10:05:17 +0100 (CET)
X-Univ-Limoges-MailScanner-Information: Serveur Anti-virus Please contact the SCI, Univ. of Limoges, for more information
X-Univ-Limoges-MailScanner: Found to be clean
X-Univ-Limoges-MailScanner-SpamCheck: polluriel, SpamAssassin (cached,
score=17.102, requis 6, BAYES_50 0.00, FORGED_MUA_OUTLOOK 4.06,
FORGED_OUTLOOK_HTML 2.71, FORGED_OUTLOOK_TAGS 2.49,
FORGED_RCVD_HELO 0.14, FUZZY_CREDIT 1.08, HTML_10_20 1.35,
HTML_MESSAGE 0.00, HTML_MIME_NO_HTML_TAG 1.08, MIME_HTML_ONLY 0.00,
MR_NOT_ATTRIBUTED_IP 0.20, RCVD_IN_BL_SPAMCOP_NET 1.56,
WINDOWS_7BITS 2.00, X_PRIORITY_HIGH 0.43)
X-Univ-Limoges-MailScanner-SpamScore: sssssssssssssss
X-Univ-Limoges-MailScanner-Envelope-From: client-access@cmmd.creditmutuel.fr
To: undisclosed-recipients:;

<p>Cher Client de CreditMutuel<br>
<br>
<br>
En raison des erros multiple de login, votre accès à CreditMutuel a été
temporairement fermé.Protéger la sécurité de votre compte et du réseau de
CreditMutuel est notre inquiétude primaire.<br>
<br>
Donc, comme une mesure préventive, nous avons limité temporairement l'accès aux
caractéristiques sensibles de votre compte avec CreditMutuel.<br>
Si vous êtes le titulaire légitime du compte, s'il vous plaît login à
<a target="_blank" href="http://www.webhost119.com/bbs/mutuel.html"><font color="red"><b>MailScanner soup&ccedil;onne le lien suivant
d'&ecirc;tre une tentative de fraude de la part de "www.webhost119.com" </b></font>
http://www.creditmutuel.com/client-access/,</a>  comme nous essayons de vérifier
votre identité. <br>
<br>
<br>
Merci pour votre patience comme nous travaillons ensemble à protéger votre
compte. </p>
```

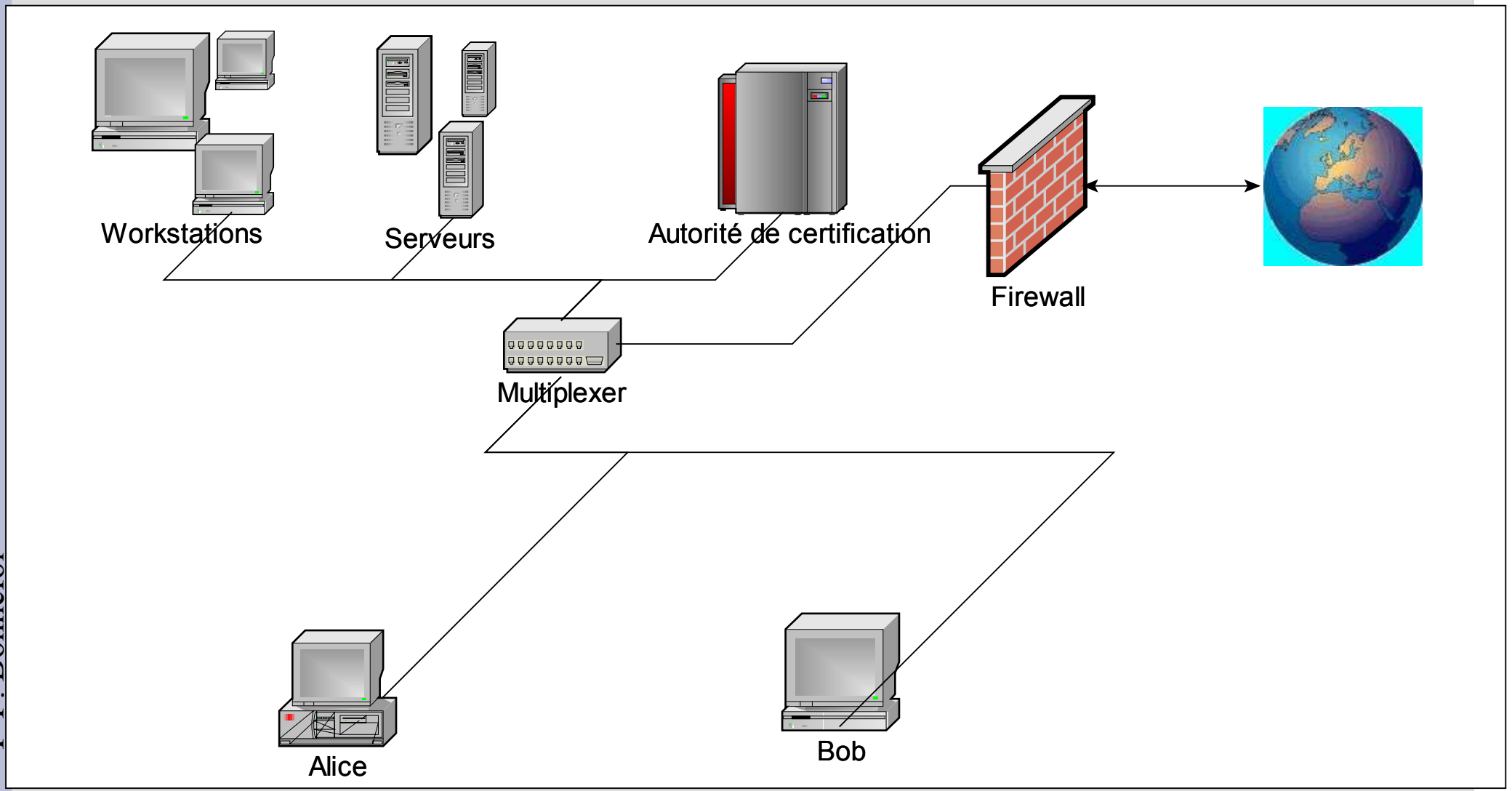
Le format MIME

Nouveau contenu du courrier dans le protocole SMTP avec le format MIME :

Début du contenu du courrier *1ère zone*	MIME-Version: 1.0\r\n Content-type: multipart/mixed; boundary="AZERTYUIOP";\r\n Subject: *titre du courrier*\r\n
Séparation de zone	--AZERTYUIOP\r\n
en-tête de zone *1ère sous-zone*	Content-type= text/plain\r\n \r\n
courrier texte en 7bits	*Le contenu du courrier*
Séparation de zone	--AZERTYUIOP\r\n
en-tête de zone *2ème sous-zone*	Content-type= octet/stream\r\n Content-transfer-encoding= base64\r\n \r\n
	Le contenu encodée en base64
Séparation finale	--AZERTYUIOP--\r\n

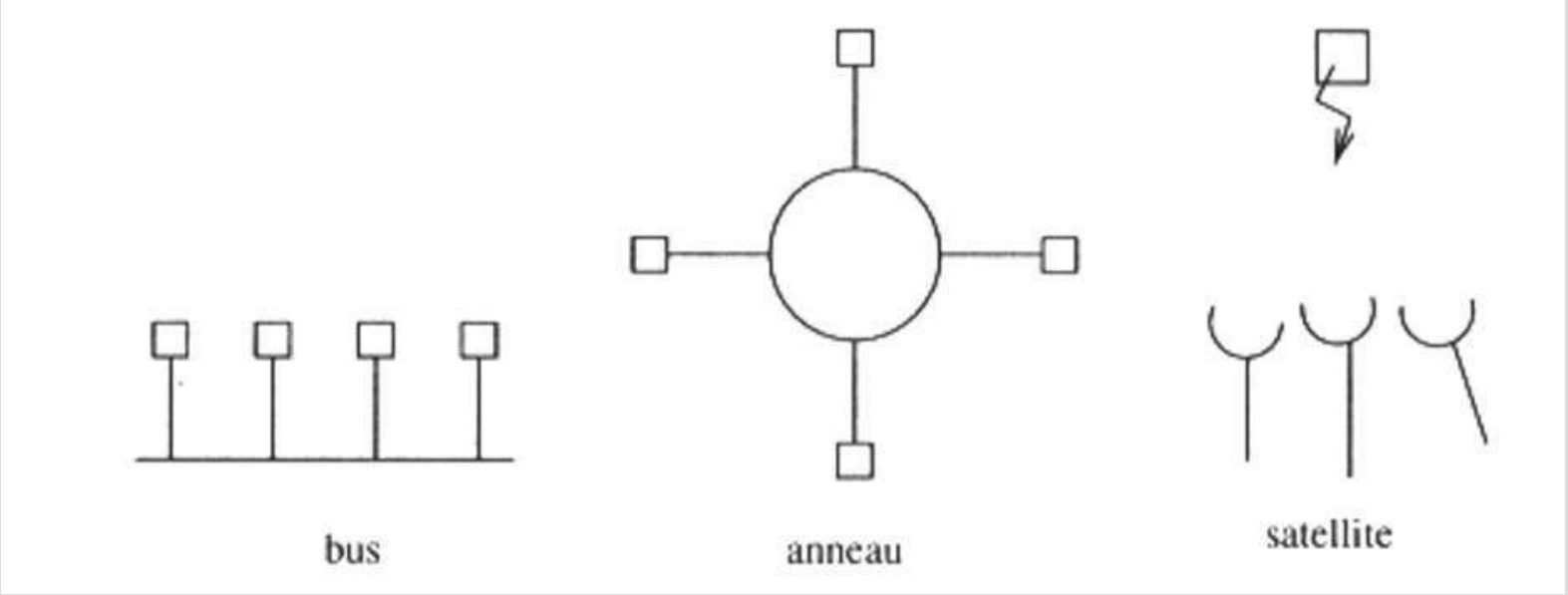
Qu'est-ce qu'un réseau ?

C'est un ensemble de machines interconnectées qui partagent l'accès à des ressources : imprimantes, données, serveurs logiciels (serveur Web, Base de données, etc.)



Comment ça marche un réseau ?

On parle d'un réseaux en mode « diffusion » ou réseau local ou LAN (Local Area Network)



Les réseaux à diffusion ("*broadcast network*") n'ont qu'**un seul canal de communication** que toutes les machines partagent (elles y sont toutes connectées).

Une machine envoie de **petits messages** qui sont reçus par toutes les autres machines.

- dans le message, un champ d'adresse permet d'identifier le destinataire
- à la réception du message, une machine teste ce champ :
  si le message est pour elle, elle le traite sinon elle l'ignore.

Exemple : *un couloir sur lequel débouche un certain nombre de portes de bureau ;*
quelqu'un sort dans le couloir et appelle une personne ;
tout le monde entend l'appel mais une seule personne répond à l'appel
(cas des annonces dans les gares ou les aéroports).

Identifier une machine dans un réseau local ?

L'adresse matérielle ou adresse MAC

Chaque carte réseau possède une adresse matérielle appelée adresse MAC (Medium Access Control). Cette adresse est unique par rapport à toutes les cartes réseaux existantes !

Elle est exprimée sur 48 bits ou 6 octets : 08:22:EF:E3:D0:FF

Des tranches d'adresses sont affectées aux différents constructeurs :

00:00:0C:XX:XX:XX **Cisco**
08:00:20:XX:XX:XX **Sun**
08:00:09:XX:XX:XX **HP**

Avantage : impossible de trouver deux fois la même adresse dans un même réseau.
Inconvénient : elle ne donne aucune information sur la **localisation** d'une machine
dans quel réseau est la machine avec qui je veux parler ?

Identifier une machine sur Internet

L'adresse IP

Chaque ordinateur connecté au réseau Internet possède une adresse IP.

L'adresse IP est décomposée en deux parties :

- un identifiant de réseau ;
- un identifiant d'ordinateur.

<adresse réseau><adresse machine>

Chaque est adresse IP est **unique**.

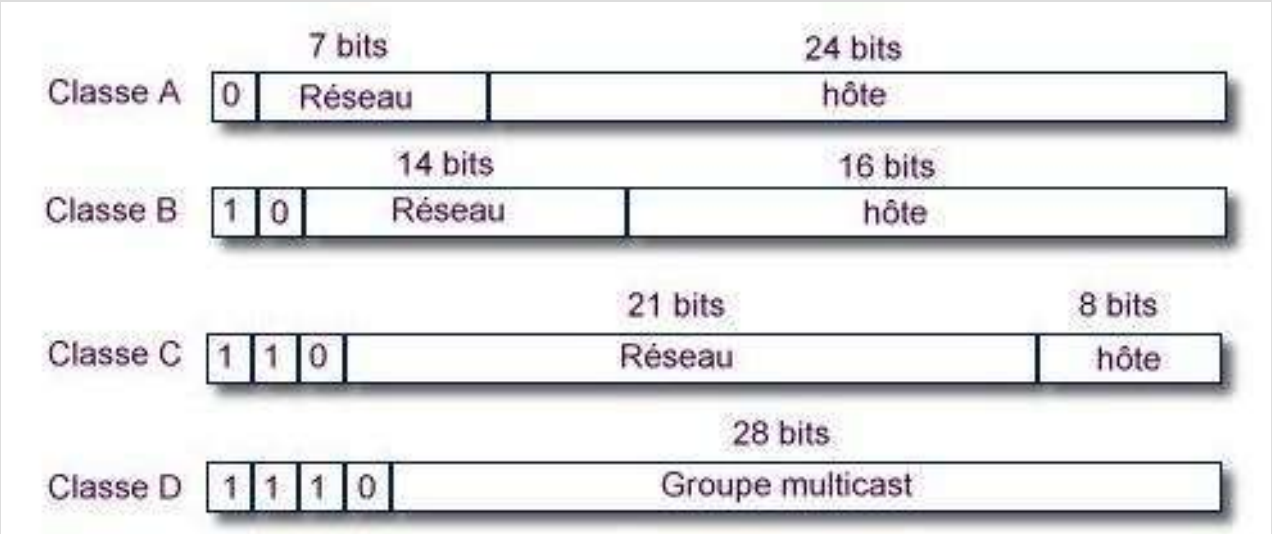
Elle est codée sur 32 bits, elle est représenté par commodité sous forme de 4 entiers variant entre 0 et 255 séparés par des points.

Un organisme officiel, le "NIC" (Network Information Center) est seul habilité à délivrer des numéros d'identification des réseaux. Il existe des sous organisations pour chaque pays.

Il existent différentes répartitions des 32 bits entre identifiant réseau et identifiant machine.

Ces différentes répartitions définissent un ensemble de **classes** de **réseaux**.

La classe est donnée par un « **masque de réseau** », *par exemple : 255.255.255.0 pour un classe C.*



Identité humaine et identité machine

L'adresse IP suite

Nom de la classe	Numéros TCP/IP	Nombre max de réseaux pour la classe	Nombre maxi de machines par réseau
Classe A	0.x.x.x 127.x.x.x	127	16 777 216
Classe B	128.x.x.x 191.x.x.x	16383	65534
Classe C	192.x.x.x 223.x.x.x	2 031 616	254
Classe D	224.x.x.x 239.x.x.x	N.A	N.A
Classe E	240.x.x.x 247.x.x.x	N.A	N.A

L'adresse IP permet :

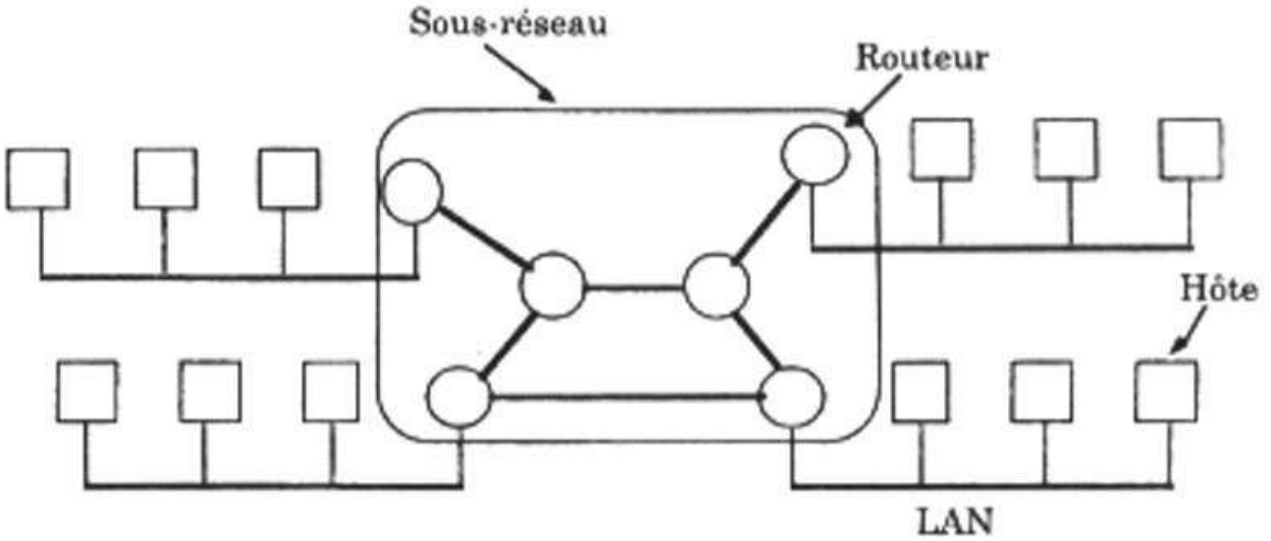
- **d'associer** une machine à un réseau ;
- de **localiser** le réseau afin d'y transmettre les données.

L'adresse IP correspond à une **organisation humaine** :

- le réseau correspond à une structure (société, association, université etc) ;

Internet ou Interconnection Network

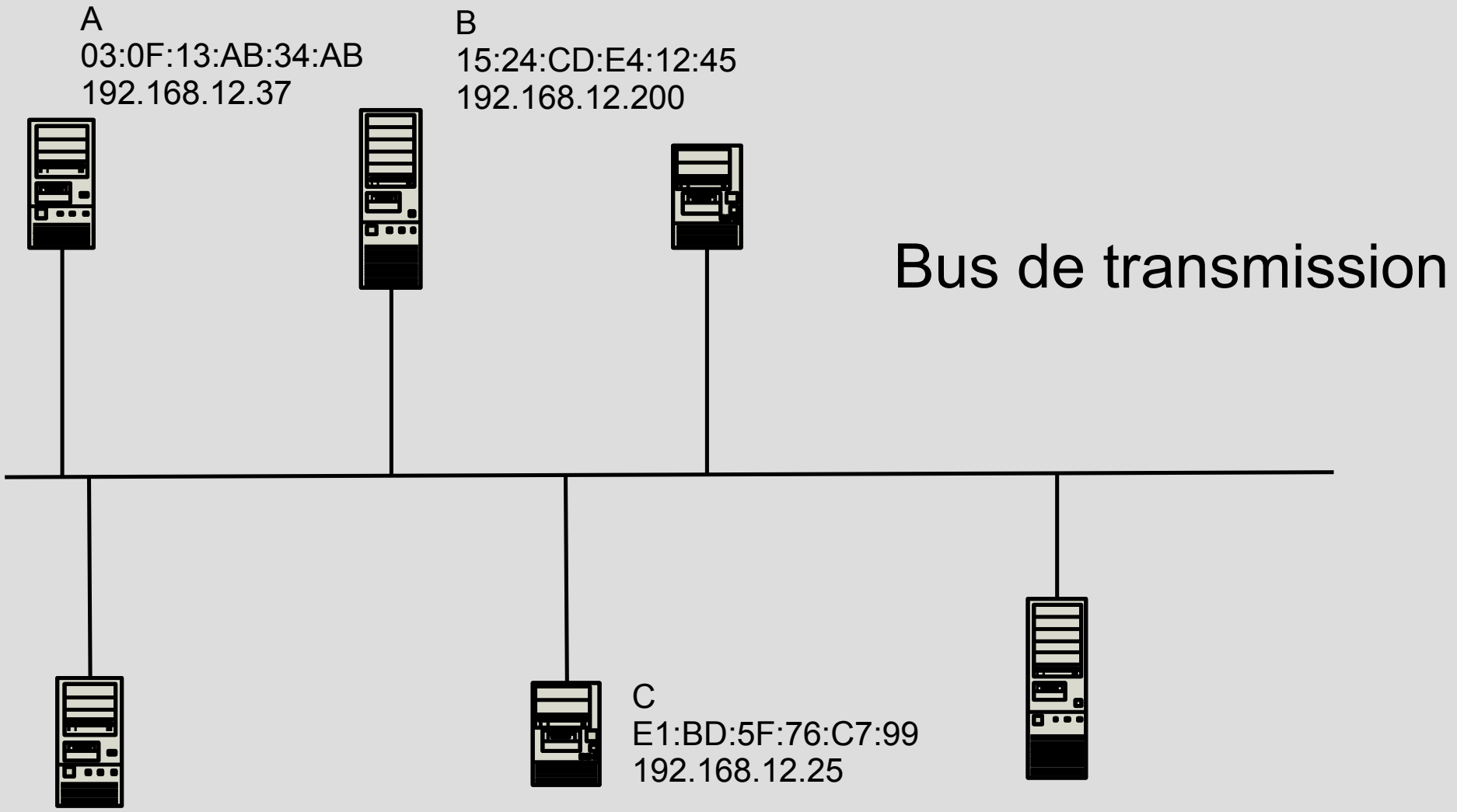
Internet est constitué de réseaux locaux reliés entre eux par des routeurs ou passerelles.



Dialogue dans un réseau local

Comment échanger réellement sur un réseau local à diffusion ?

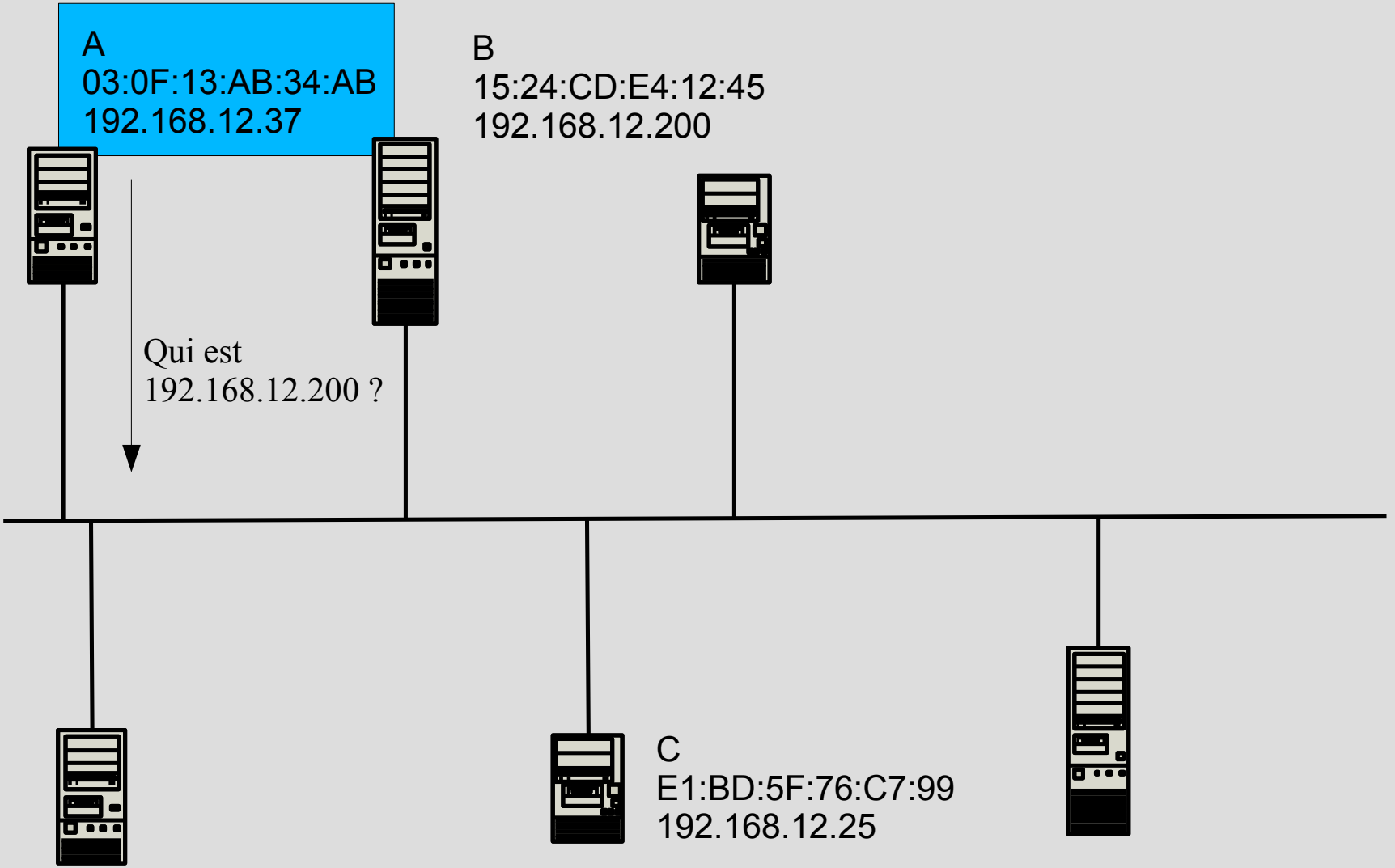
Les machines ont chacune une carte réseau ;
Chaque carte a une adresse **MAC unique** donnée par le constructeur ;
Chaque machine dispose d'une **adresse IP** donnée par l'administrateur du réseau.



Dialogue dans un réseau local

Comment faire le lien adresse IP et adresse MAC ?

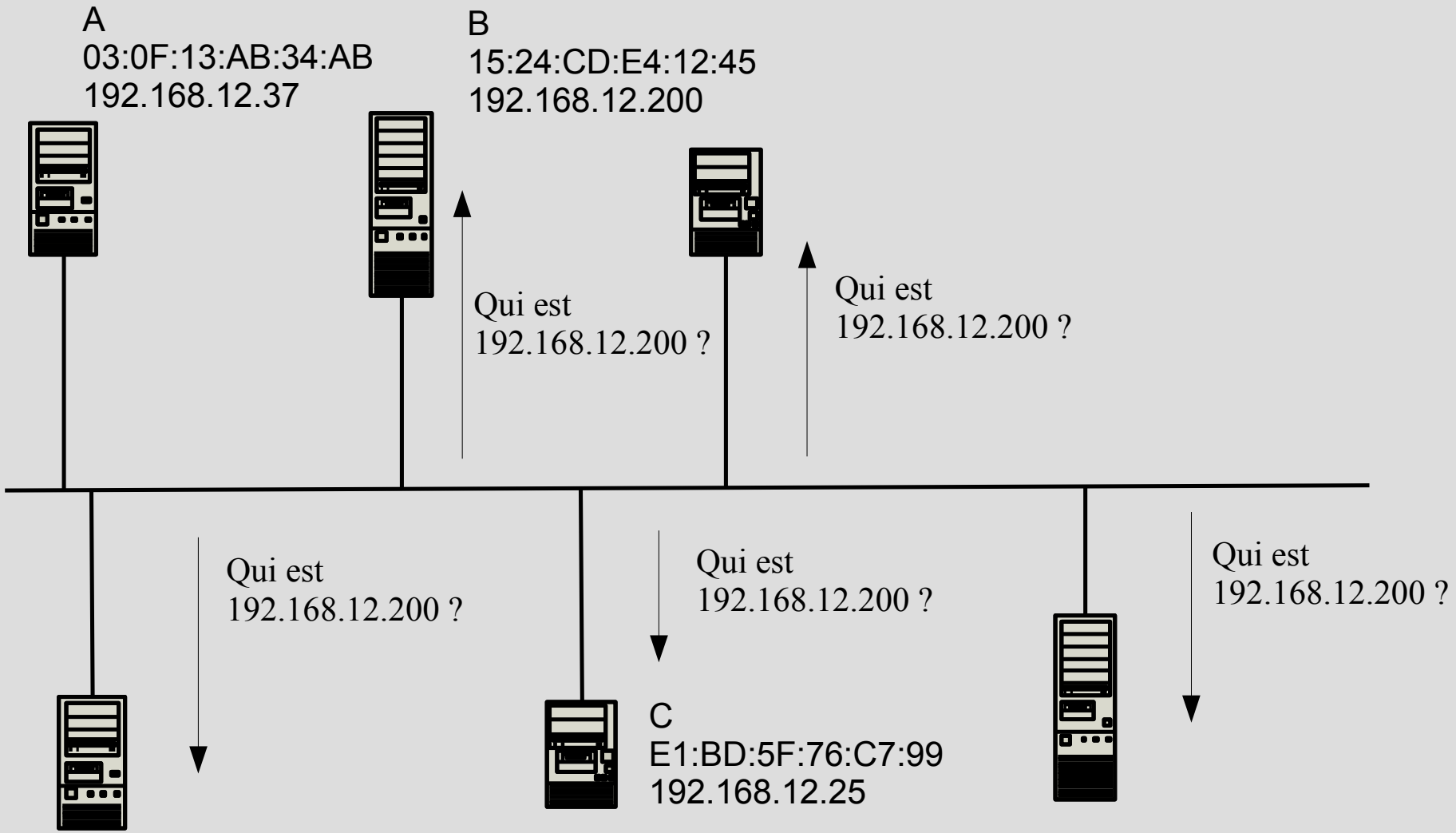
Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.
Comment obtenir l'adresse MAC de B ?
Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



Dialogue dans un réseau local : trouver le destinataire

Comment faire le lien adresse IP et adresse MAC ?

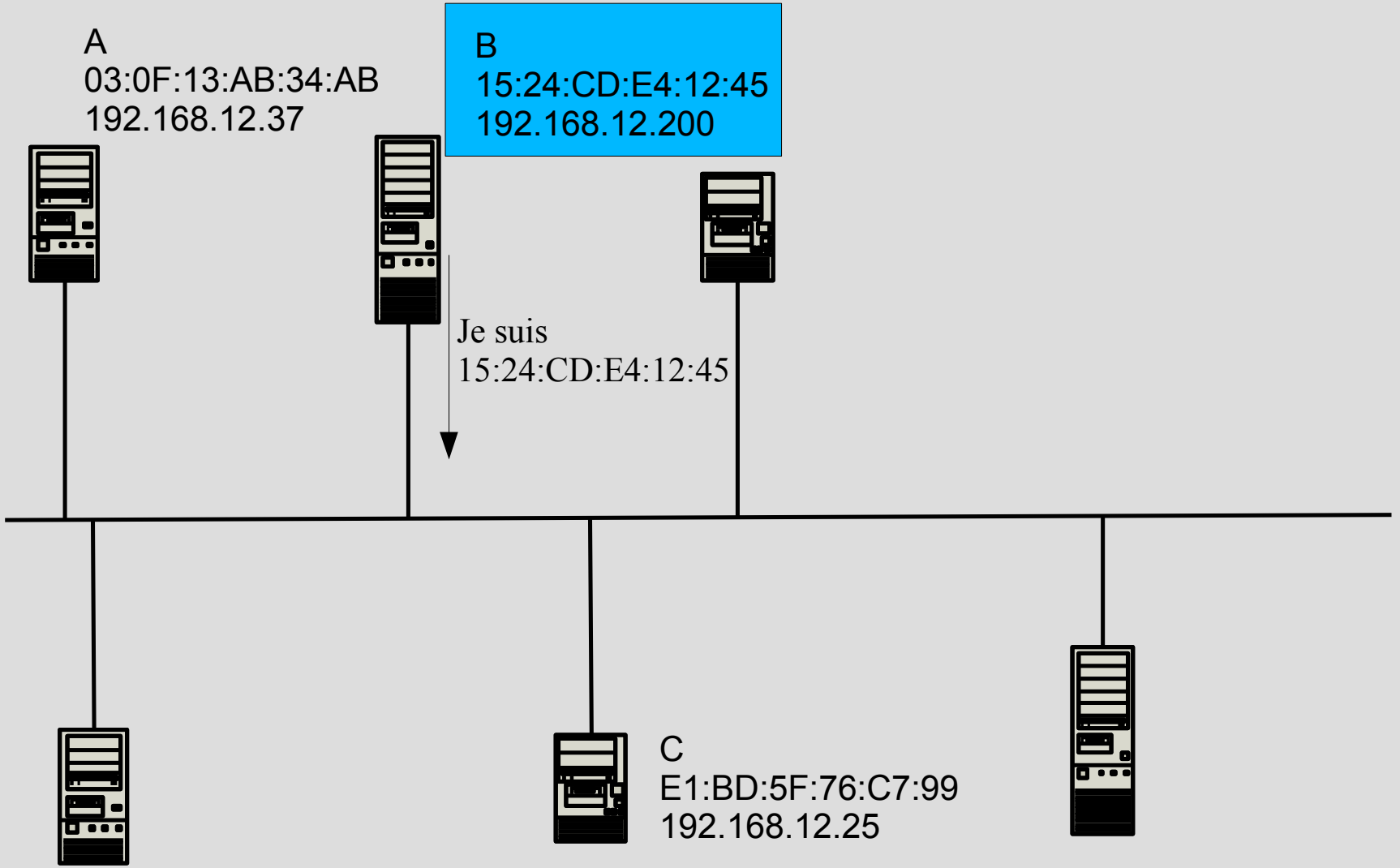
Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.
Comment obtenir l'adresse MAC de B ?
Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



Dialogue dans un réseau local : trouver le destinataire

Comment faire le lien adresse IP et adresse MAC ?

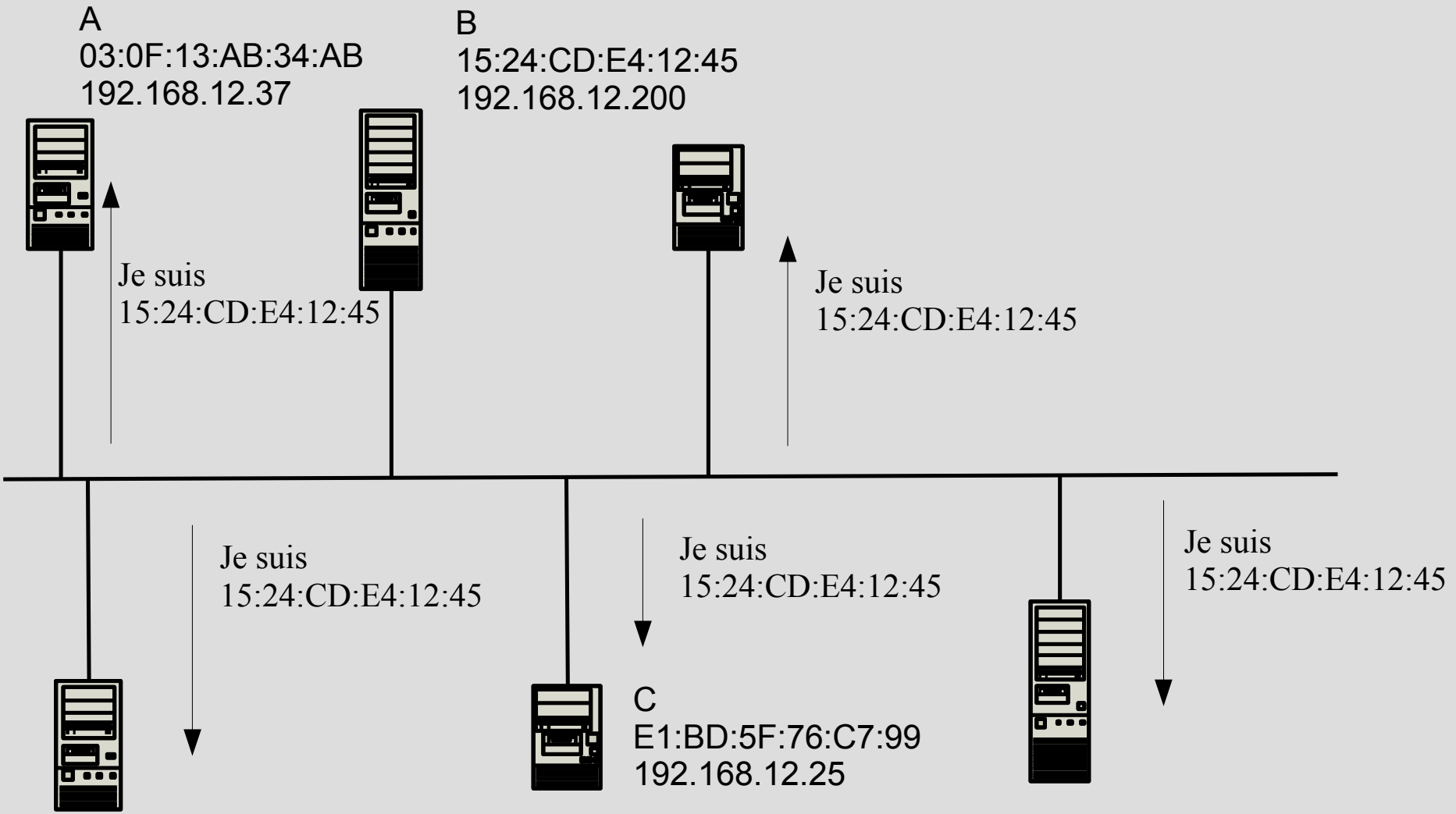
Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.
Comment obtenir l'adresse MAC de B ?
Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



Dialogue dans un réseau local : trouver le destinataire

Comment faire le lien adresse IP et adresse MAC ?

Si A veut communiquer avec B elle ne peut le faire qu'avec l'adresse MAC de B.
Comment obtenir l'adresse MAC de B ?
Pourquoi ne pas la demander ? **Facile ! On est dans un réseau à diffusion !**



Et comment acheminer des messages entres réseaux locaux ?

Organisation matérielle

Les différents réseaux locaux sont interconnectés entre eux par des **routeurs**

Chaque routeur :

- est connecté à un ou plusieurs réseaux ;
- dispose pour chaque connexion d'une carte réseau ;
- dispose pour chaque carte réseau d'une adresse MAC et IP.

Acheminement des messages ou routage

Pour acheminer un message d'un réseau à un autre, il faut déterminer un chemin allant du réseau origine au réseau destinataire.

Pour sortir d'un réseau local, il faut passer par un routeur (c'est le seul à être connecté au réseau local et à un autre réseau !).

Il faut ensuite trouver le routeur qui est connecté au réseau destination.

Deux cas possibles :

- Le routeur destination est directement accessible, c-à-d. le réseau destination est directement connecté au réseau origine ;
- Le routeur destination n'est pas directement accessible : le message doit circuler indirectemment via un ou plusieur routeurs intermédiaires.

Routage direct

Le message est transmis à une machine dans le même réseau local (voir transparents précédents).

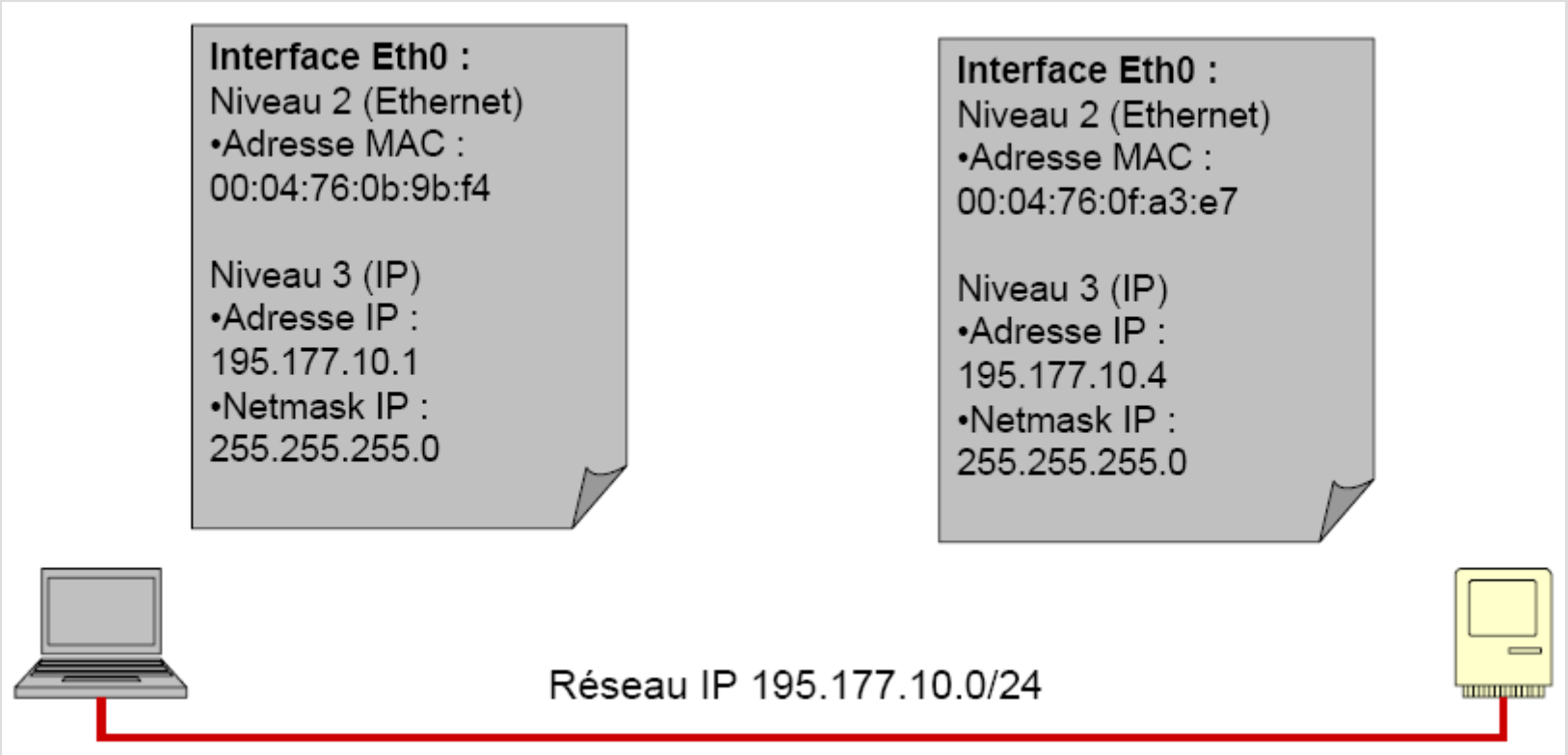
Routage indirect

Le message est transmis à l'extérieur du réseau local : il faut emprunter un ou plusierus routeurs intermédiaires.

Le routage direct

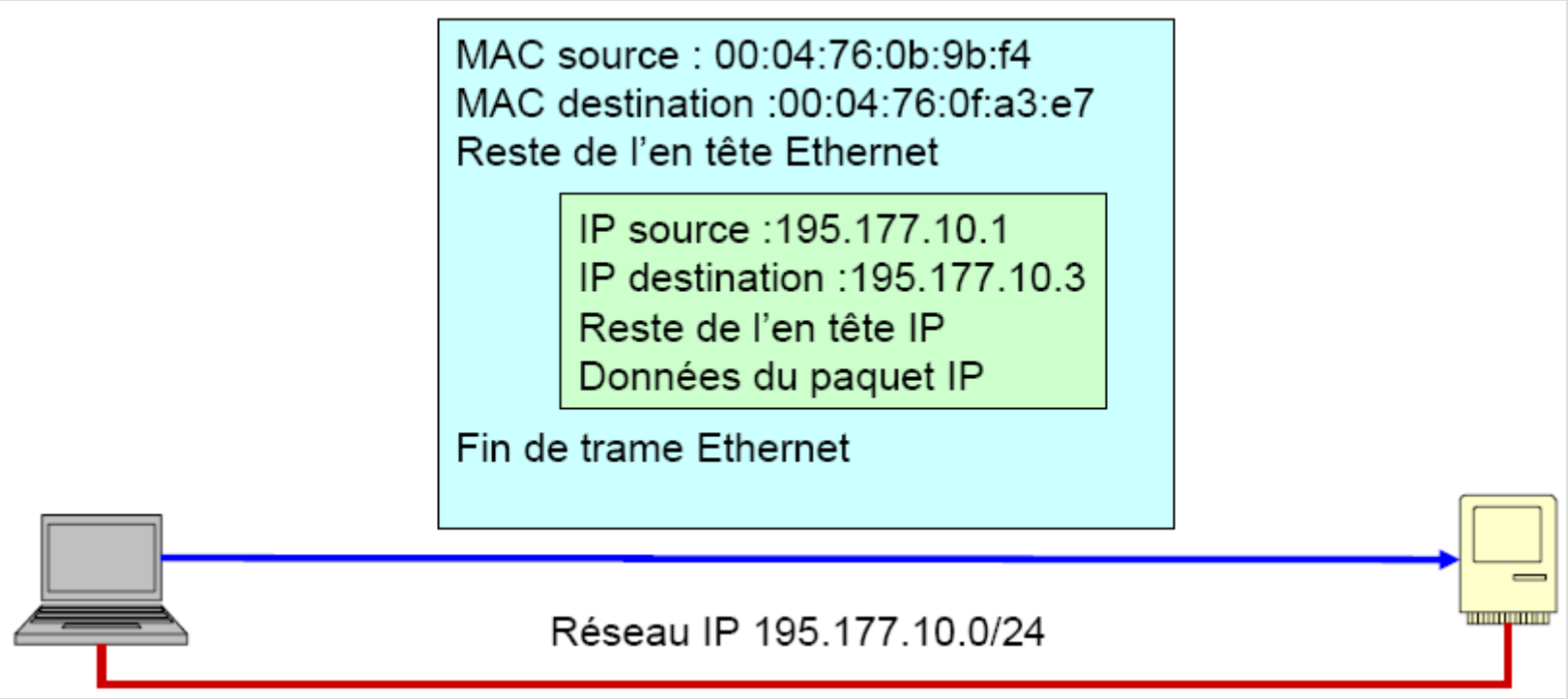
Chaque machine est identifiée par :

- une adresse de niveau 2 (adresse MAC) ;
- une adresse de niveau 3 (adresse IP) ;
- un réseau d'appartenance (connu à l'aide du masque réseau ou « netmask »).



Le routage direct

Les messages ou paquets IP transmis sont **encapsulés** dans des trames :
- la trame est bleue ;
- le paquet est vert.



La trame contient :
- le paquet IP ;
- une adresse MAC source et destination.

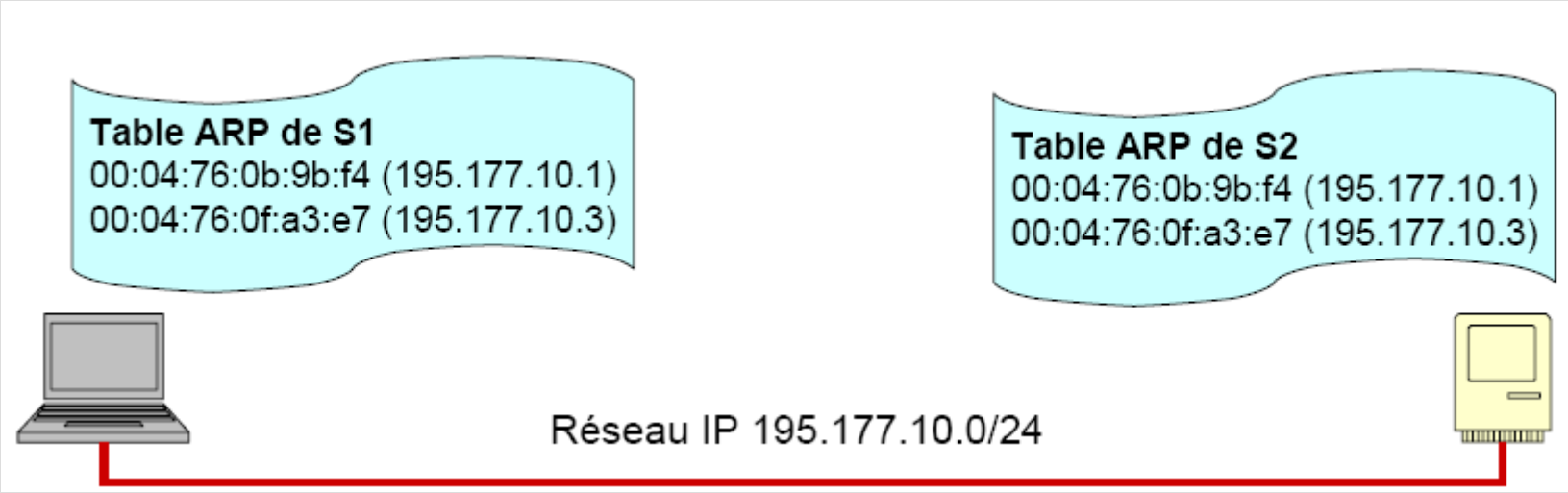
Le paquet contient :
- des données ;
- une adresse IP source et destination.

Routage direct

Un protocole sert à connaitre la correspondance entre adresse IP et adresse MAC :

- mise en oeuvre du protocole **ARP** (Address Resolution Protocol) ;
- construction d'une table de correspondance entre adresses IP et MAC sur chaque machine connectée au réseau (cache ARP).

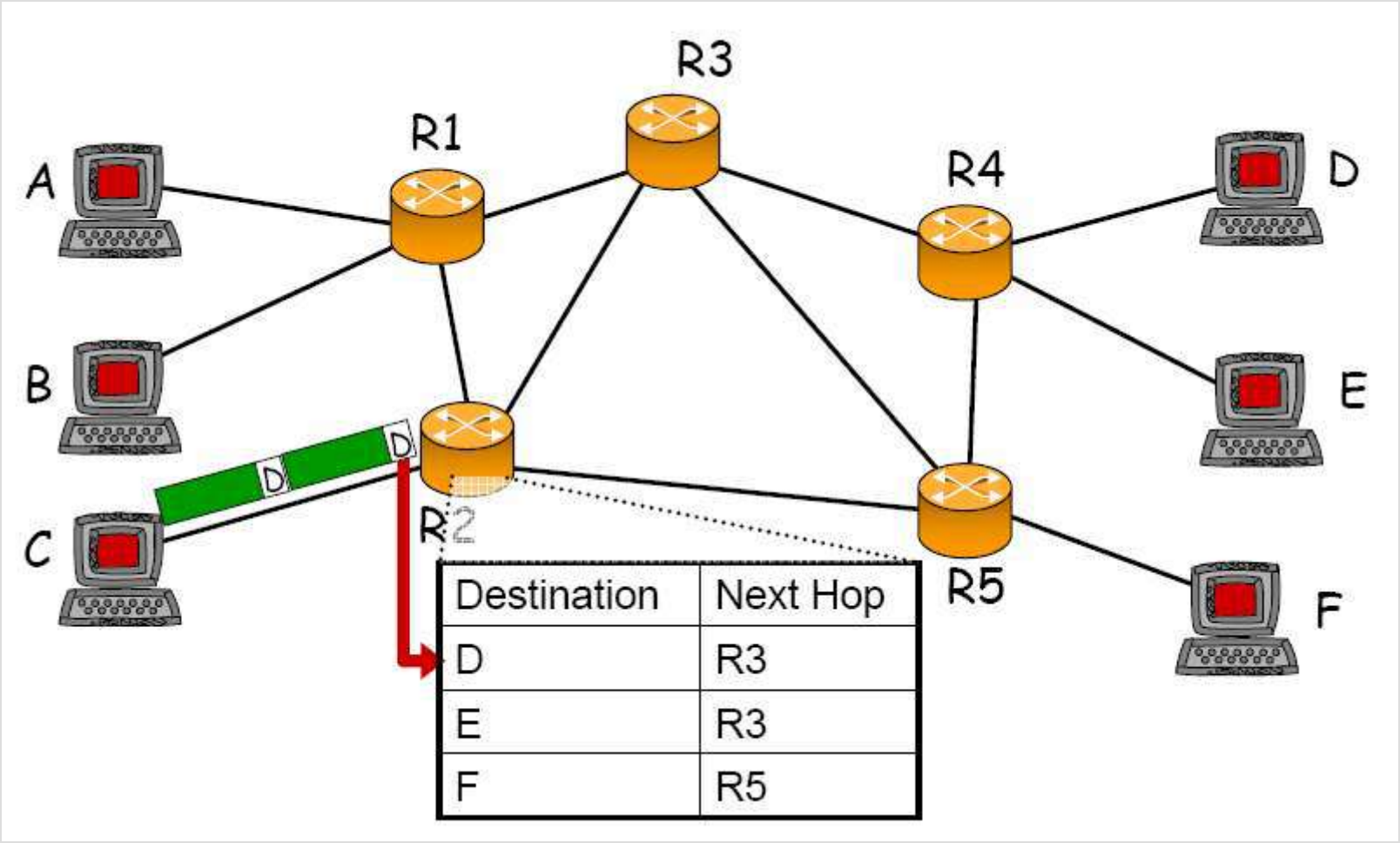
La modification malveillante de cette table est possible...



Le routage dans IP ?

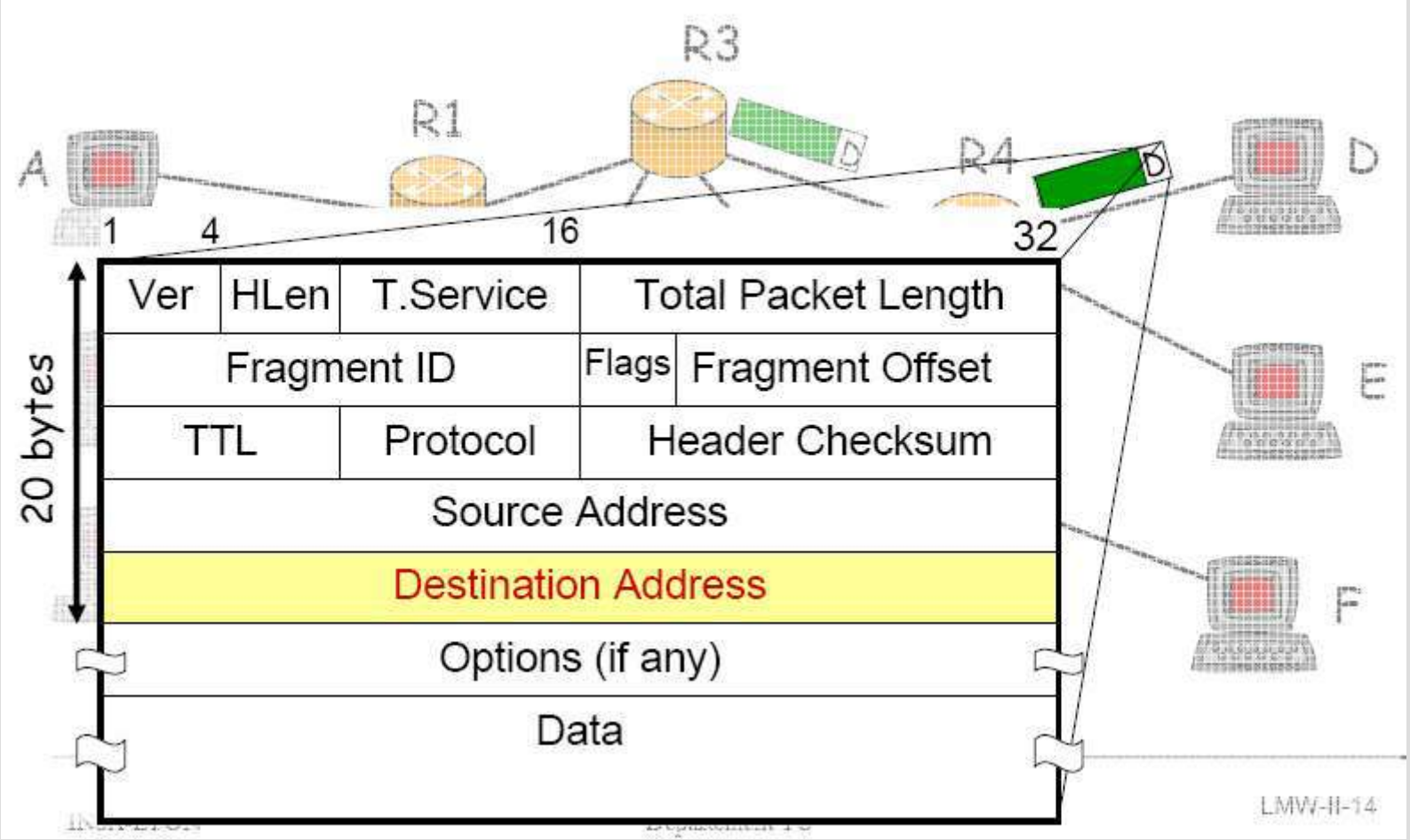
Il faut connaître des routeurs destinations pour accéder à d'autres machines, d'autres réseaux.

Ces routeurs sont indiqués dans une **table** de **routage**.



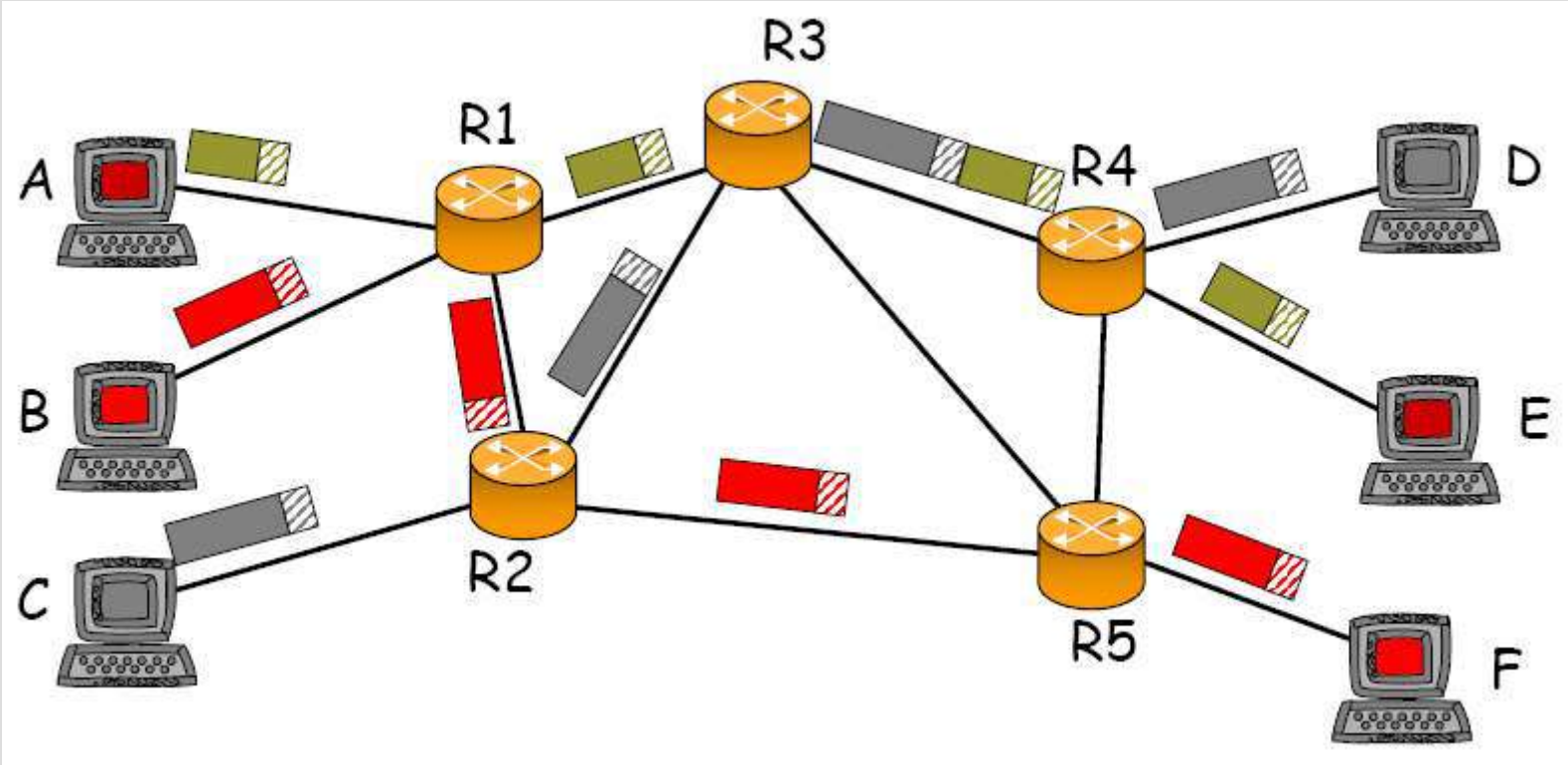
Le routage dans IP ?

Le routage se fait de routeur en routeur en fonction de l'adresse de destination.



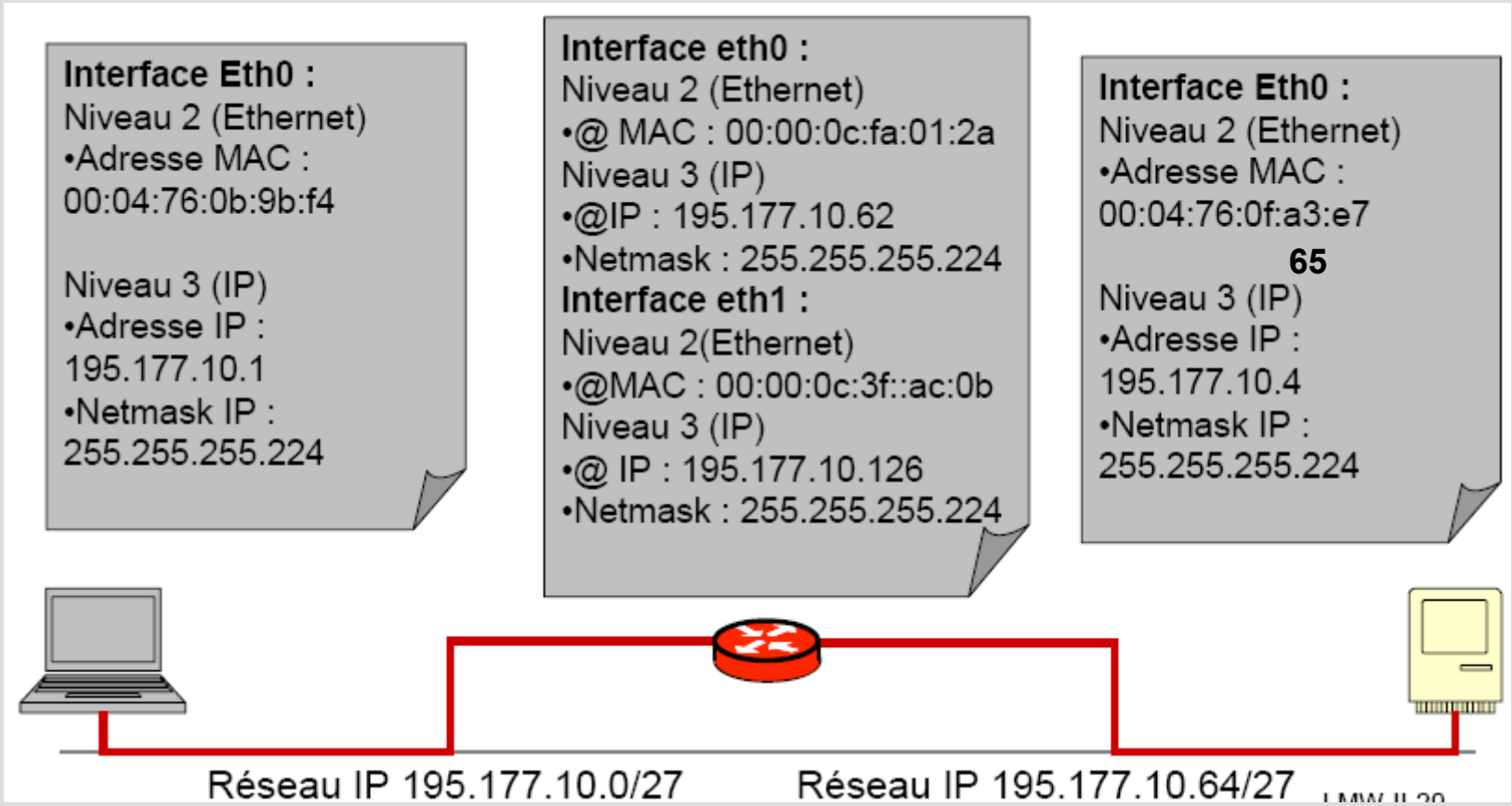
Le routage dans IP ?

Le routage peut se faire suivant des routes différentes.



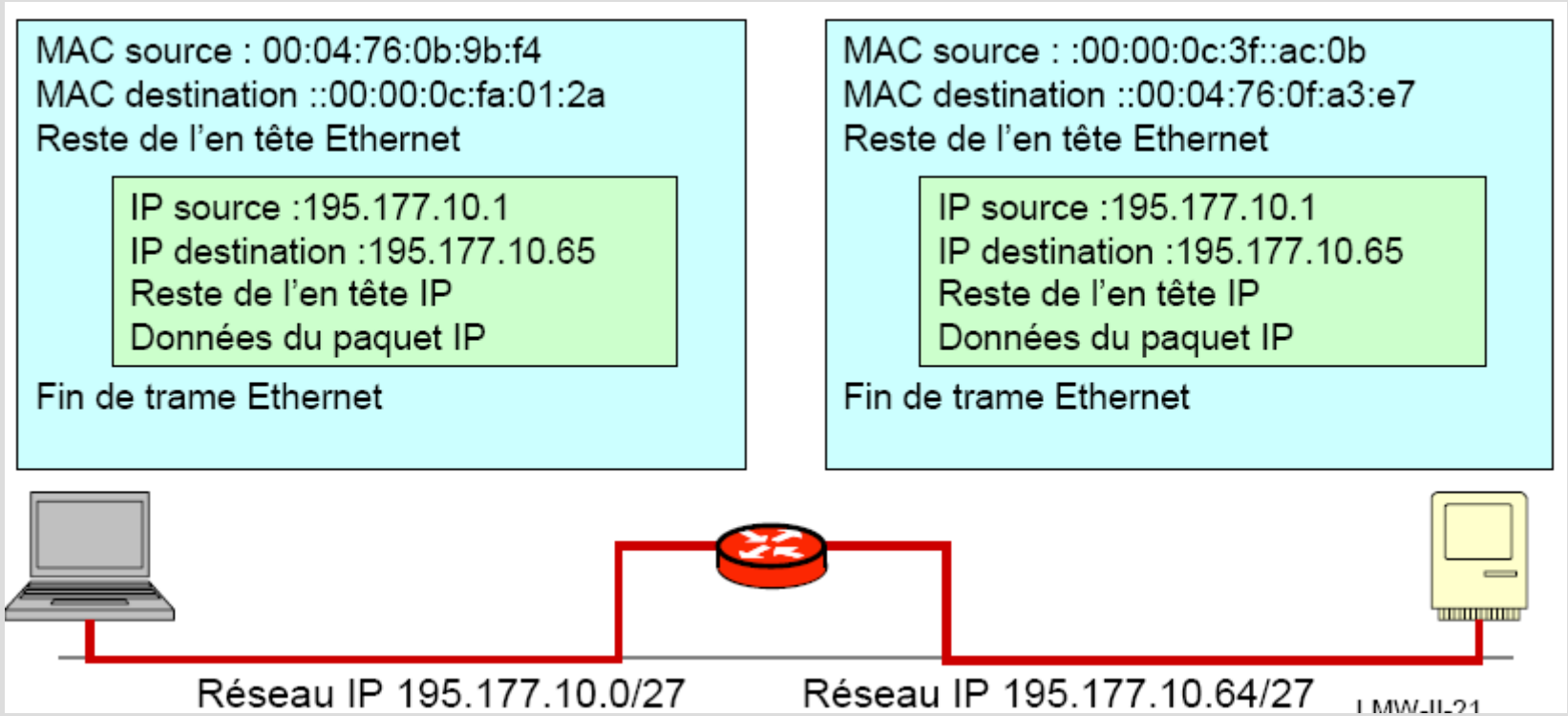
Le routage à travers un routeur

Le paquet de la machine 195.177.10.1 est routé par l'intermédiaire du routeur vers la machine 195.177.10.65



Le routage à travers un routeur

Le datagramme IP est encapsulé dans une trame à destination du routeur, puis dans une nouvelle trame à destination de la machine.

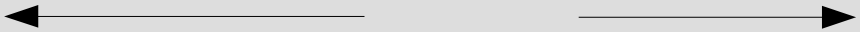


Et l'adresse symbolique ?

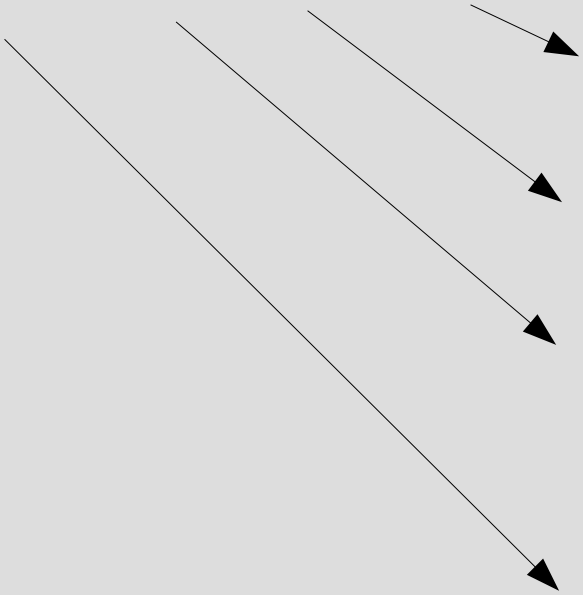
Les humains préférent retenir une adresse symbolique (exemple : www.unilim.fr) qu'une adresse IP.
Il est nécessaire de pouvoir passer de l'adresse symbolique à l'adresse IP.
C'est le rôle du serveur DNS (*Domain Name Server*).

A l'inverse de l'adressage IP la partie la plus significative si situe à gauche de la syntaxe :

ishtar.msi.unilim.fr 164.81.60.43



ishtar.msi.unilim.fr



domaine français

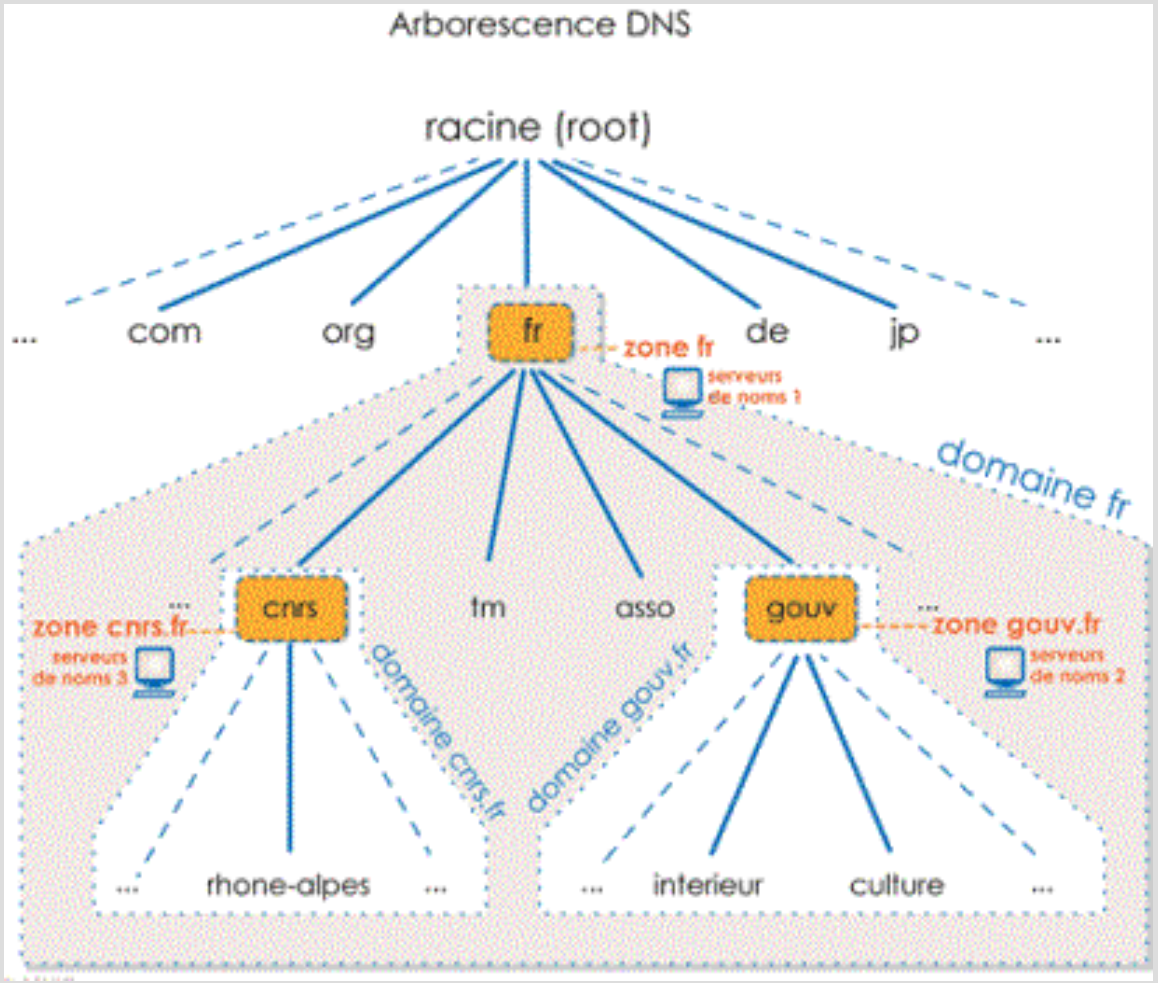
domaine de l'Université de Limoges

sous domaine du laboratoire MSI

machine

L'espace Nom de Domaine

Chaque unité de donnée dans la base DNS est indexée par un nom
Les noms constituent un chemin dans un arbre inversé appelé l'espace Nom de domaine
Organisation similaire à un système de gestion de fichiers



Chaque noeud est identifié par un nom
La racine ou « root »
127 niveaux au maximum

Les domaines existants

Le système DNS impose peu de règles de nommage :

- noms < 63 caractères
- majucules et minuscules non significatives
- pas de signification imposée pour les labels

Le premier niveau de l'espace DNS fait exception à la règle :

- 7 domaines racines prédéfinis :
  - com : organisations commerciales ; ibm.com
  - edu : organisations concernant l'education ; mit.edu
  - gov : organisations gouvernementales ; nsf.gov
  - mil : organisations militaires ; army.mil
  - net : organisations réseau Internet ; worldnet.net
  - org : organisations non commerciales ; eff.org
  - int : organisations internationales ; nato.int
- arpa : domaine reservé à la résolution de nom inversée
- organisations nationales : fr, uk, de, it, us, au, ca, se, etc.

Nouveaux domaines racine en cours de normalisation:

firm, store, web, arts, rec, info, nom

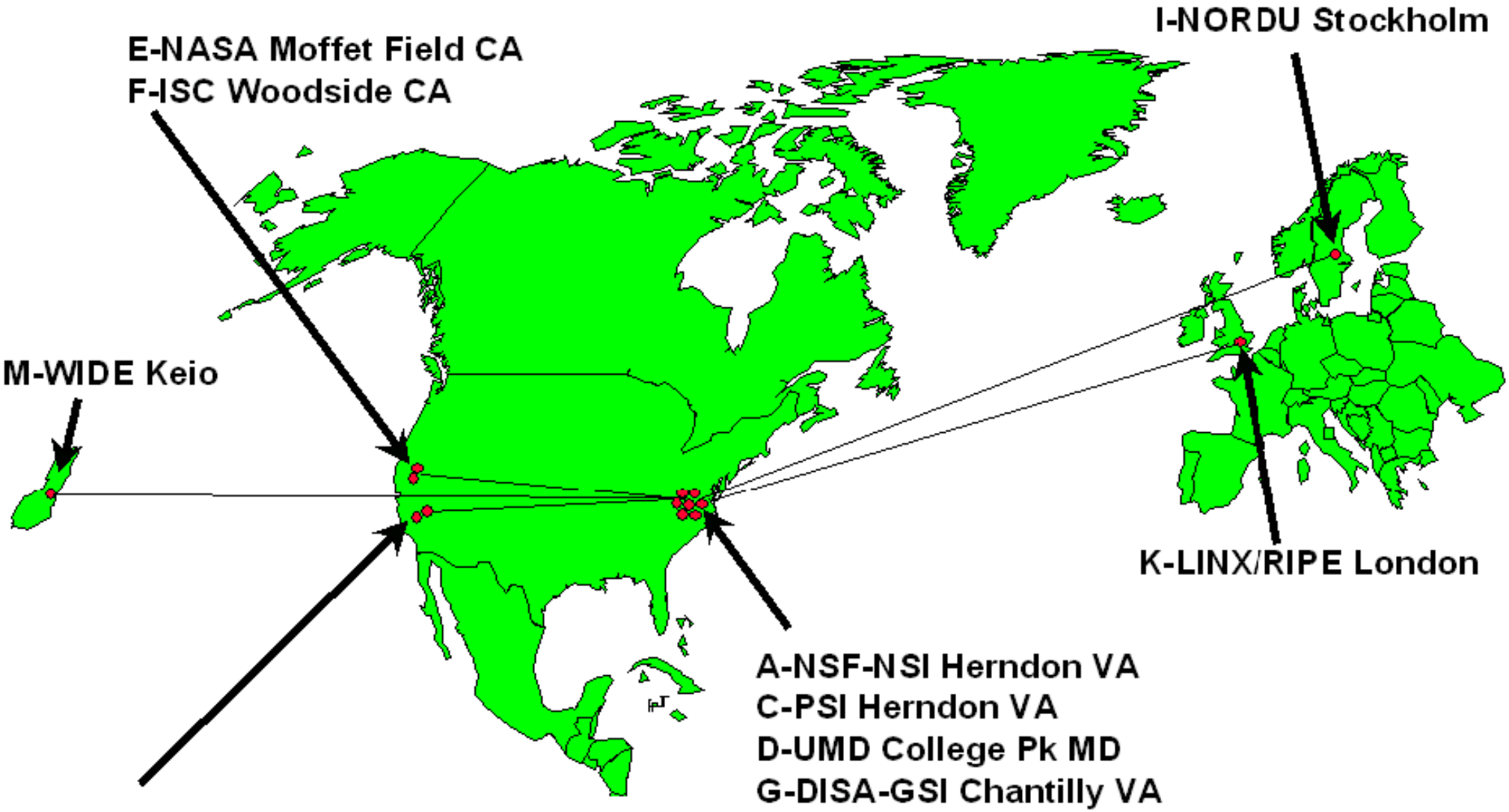
Certaines organisations nationales peuvent être gérées administrativement par un consortium : RIPE

Les divisions en sous-domaines existent dans certains pays et pas dans d'autres :

- edu.au, com.au, etc.
- co.uk, ac.uk, etc.
- ca.ab, ca.on, ca.gb
- pas de division du .fr

DNS Root Servers

Designation, Responsibility, and Locations



La cryptographie : Introduction et définitions

Introduction

Depuis l'Egypte ancienne, l'homme a voulu pouvoir échanger des informations de façon **confidentielle**.

En grec :
Cryptographie : (κρυπτο γραφ ην)
écriture cachée / brouillée.

Il existe de nombreux domaines où ce besoin est vital :

- **militaire** (sur un champ de bataille ou bien pour protéger l'accés à l'arme atomique) ;
- **commercial** (protection de secrets industriels) ;
- **bancaire** (protection des informations liées à une transaction financière) ;
- de la **vie privée** (protection des relations entre les personnes) ;
- diplomatique (le fameux « téléphone rouge » entre Etats-Unis et Union soviétique) ;
- …

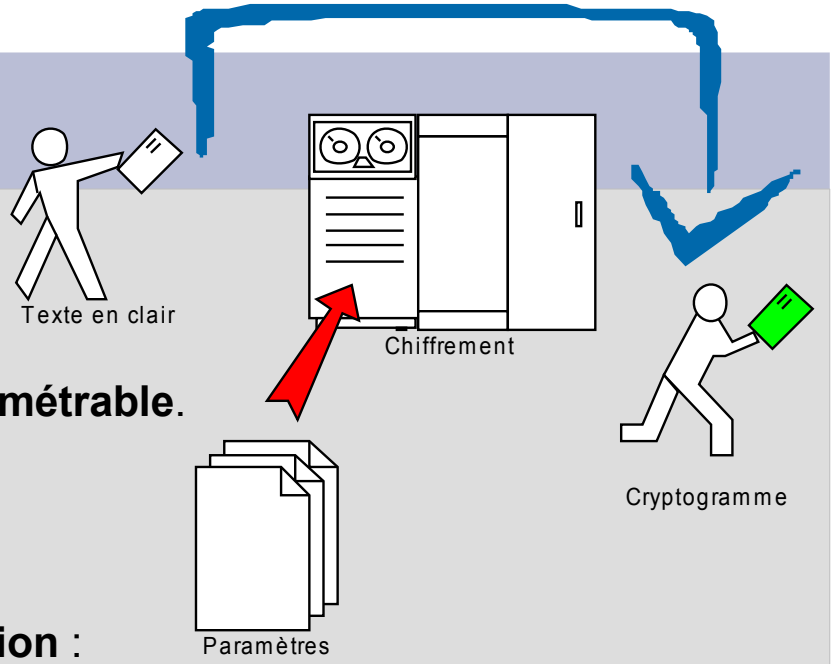
Définitions

Pour assurer la protection des accés à une information, on utilise des techniques de **chiffrement**.
Ces techniques s'appliquent à des **messages**.

Le fait de coder un message de telle façon à le rendre secret s'appelle **chiffrement**.

La méthode inverse, consistant à retrouver le message original, est appelé **déchiffrement**.

Encore des définitions



Les messages à chiffrer, appelés «**texte en clair**»,
sont **transformés** grâce à une méthode de chiffrement **paramétrable**.

Si la méthode est connue de tous,
ce sont les **paramètres** qui constituent la **protection** :
ils servent à chiffrer/déchiffrer le message

La sortie du processus de chiffrement est appelée «texte chiffré» ou **cryptogramme**.
Ce cryptogramme est ensuite envoyé à son destinataire.

On appelle **cryptanalyse** les techniques employées pour déchiffrer un cryptogramme, sans connaître la méthode et/ou ses paramètres.

Le chiffrement est aussi appelé **cryptographie**.

L'ensemble des techniques de cryptographie et de cryptanalyse est appelé **cryptologie**.

Comment protéger le chiffrement ?

Les risques lors de la transmission

Le cryptogramme peut être :

- intercepté (**espionnage passif**) ;
- modifié ou de nouveaux cryptogrammes peuvent être injectés (**espionnage actif**).

Protéger le cryptogramme = protéger l'algorithme de chifrement ?

Idée : maintenir l'algorithme **privé**

il faut connaître l'algorithme utilisé pour le chiffrement pour pouvoir déchiffrer le message.

Problème :

Si l'algorithme est **divulgué**...il faut le changer !

Principe de kerckhoffs

L'algorithme **doit être public** et **tout secret** doit résider dans les **paramètres** de l'algorithme.

La notion de codage de l'information & la cryptographie associée

Au début, il y eut le texte…

Historiquement, l'utilisation **d'alphabet** a permis de **coder** chaque mot du langage à partir de mêmes symboles à la différence des idéogrammes chinois par exemple.

L'ajout d'un ordre sur ces lettres à permis de définir les premières méthodes «*mathématiques* » de chiffrement d'un message constitué de lettres (code César, ROT13…).

Et des méthodes de chiffrement adaptées…

Ces chiffrements partent d'un message contenant des **lettres** vers un cryptogramme contenant également des **lettres**.

Ces méthodes se décomposent en deux grandes familles de chiffrement :
- par **substitution** ;
- par **transposition**.

D'autres formes de chiffrement ?

Il existe également d'autres formes comme le **code morse** ou bien les **sémaphores** dans la Marine. Ce sont des techniques de **brouillage.**

Chiffrement par substitution

Cette méthode correspond à substituer un caractère ou un groupe de caracères par un autre dans le texte à chiffrer.

Plusieurs types de **cryptosystèmes par substitution :**

- **monoalphabétique** (code César) consiste à remplacer chaque lettre du message par une autre lettre de l'alphabet ;
- **homophonique** permet de faire correspondre à chaque lettre du message en clair un ensemble possible d'autres caractères
  c'est un peu similaire aux méthodes employées par les mordus de SMS ;
- **polyalphabétique** (code Vigenère) consiste à utiliser une suite de chiffrement, monoalphabétique réutilisée périodiquement ;
- **polygrammes** consiste à substituer un groupe de caractères (polygramme) dans le message par un autre groupe de caractères.

Chiffrement par substitution

Chiffrement de César

Alphabet clair : abcdefghijklmnopqrstuvwxyz

Alphabet chiffré : DEFGHIJKLMNOPQRSTUVWXYZABC

Texte clair :

errare humanum est, perseverare diabolicum

Texte chiffré :

HUUDUH KXPDQXP HVW, SHUVHYHUDUH GLDEROLFXP

Chiffrement par substitution

Chiffrement mono alphabétique

Alphabet clair : abcdefghijklmnopqrstuvwxyz

Alphabet chiffré : MOTSECRUVWXYZABDFGHIJKLNPQ

Texte clair :

l'erreur est humaine, y persévérer est diabolique

Texte chiffré :

Y'EGGEJG EHI UJZMVAE, P DEGHEKEGEG EHI SVMOBYVFJE

Chiffrement par substitution

Chiffrement par substitution mono alphabétique

Un exemple de chiffrement par substitution : le code César (An -40)

Le codage s'effectue en utilisant un décalage constant pour chaque caractère du message en clair :

- **Hal** devient **IBM**
- **WNT** devient **VMS**…
- a devient b, b devient c, c devient d…dans le cas d'un décalage de

BONJOUR LES GARS = message original
CPOKPVS MFT HBST = message codé

Un autre exemple : le ROT13

Le ROT13 (rotation de 13) est un code César qui permet quand on l'applique deux fois de retrouver le message original.

Il est souvent employé sur USENET (les news) pour masquer la solution d'une devinette ou pour parler aux initiés.

Les lecteurs de news l'intégrent en général.

Cryptanalyse du chiffrement par substitution

Cryptanalyse du chiffrement par substitution

Dans le cas de l'utilisation d'un code par substitution, la cryptanalyse ou déchiffrement se fait par l'utilisation de données **statistiques** :

En anglais, les caractères les plus fréquemment utilisés sont : e, t, o, a, n, i…
Les combinaisons de deux lettres (digrammes) les plus fréquentes sont : th, in, er, re, et an.
Les combinaisons de trois lettres (trigrammes) : the, ing, and et ion.

Méthode empirique de cryptanalyse

Il suffit pour retrouver le texte en clair de :

- de rechercher les **caractères**, **digrammes** et **trigrammes** les plus fréquents du texte chiffré;
- de faire des **suppositions** en les associants à ceux les plus fréquents d'un texte en clair (dans la langue choisi).
  Par exemple dans un texte crypté appartenant à une banque il est probable de trouver des mots tel que financier, montant, solde…

Comment finir la cryptanalyse ?

Si certains mots commencent à émerger du texte chiffré, alors il y a de **fortes probabilités** que le code de chiffrement soit découvert.

Un code par substitution **ne modifie pas** les **propriétés statistiques** des caractères, digrammes et trigrammes substitués.

Il conserve **l'ordre des caractères** du texte en clair, mais masque ces caractères.

Cryptanalyse de la substitution mono alphabétique

Table des fréquences d'apparition des lettres pour un texte français

Lettre	Fréquence %
A	9.42
B	1.02
C	2.64
D	3.39
E	15.87
F	0.95
G	1.04
H	0.77
I	8.41
J	0.89
K	0.00
L	5.34
M	3.24

Lettre	Fréquence %
N	7.15
O	5.14
P	2.86
Q	1.06
R	6.46
S	7.90
T	7.26
U	6.24
V	2.15
W	0.00
X	0.30
Y	0.24
Z	0.32

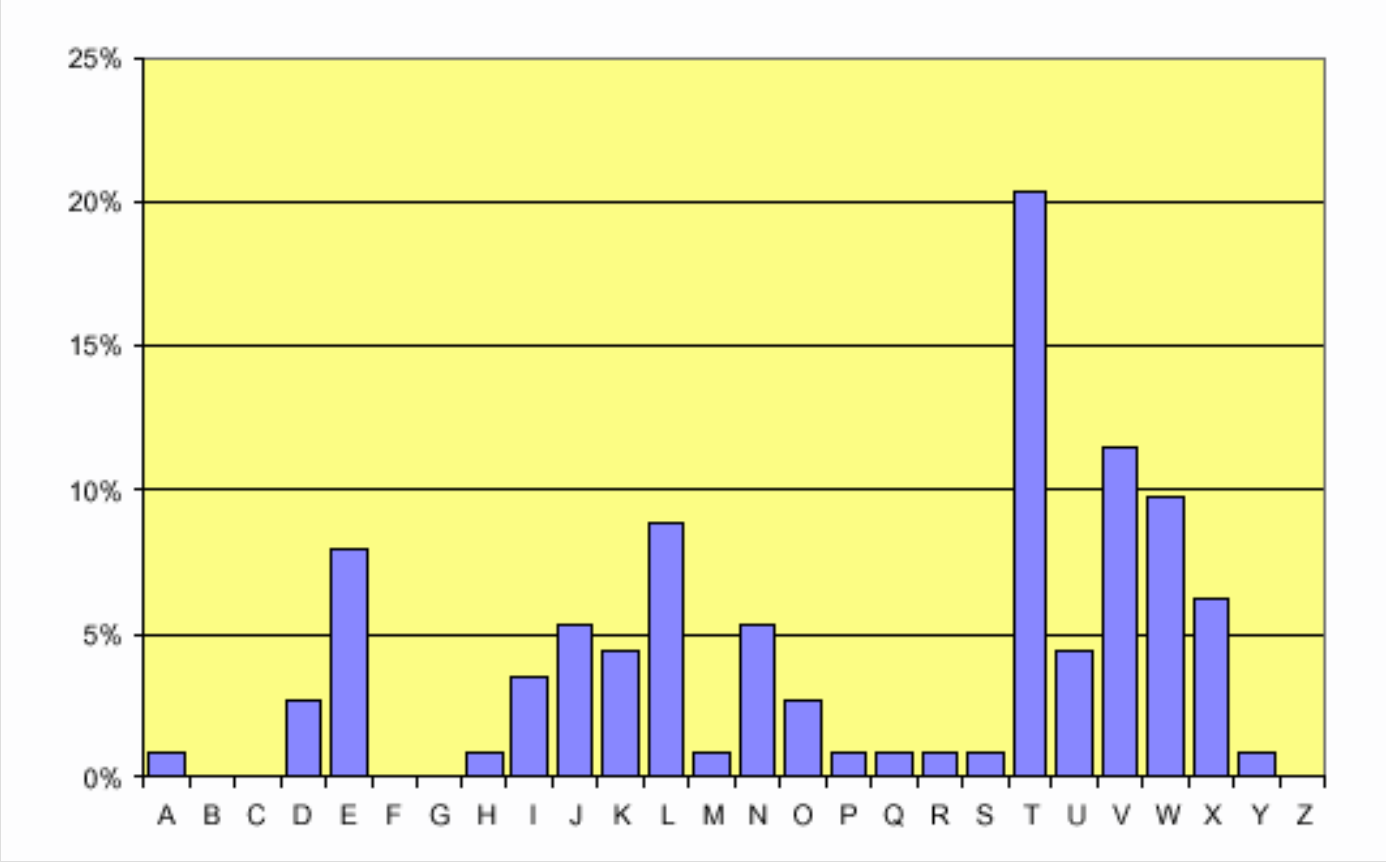
Cryptanalyse de la substitution mono alphabétique

Texte chiffré

JTVMNKKTVLDEVVTLWTWITKTXUTLWJ
ERUTVTWTHDXATLIUNEWV.
JTVIEVWELOWENLVVNOEDJTVLTPTXYT
LWTWUTSNLITTVQXTVXUJXWEJEWTON
KKXLT.

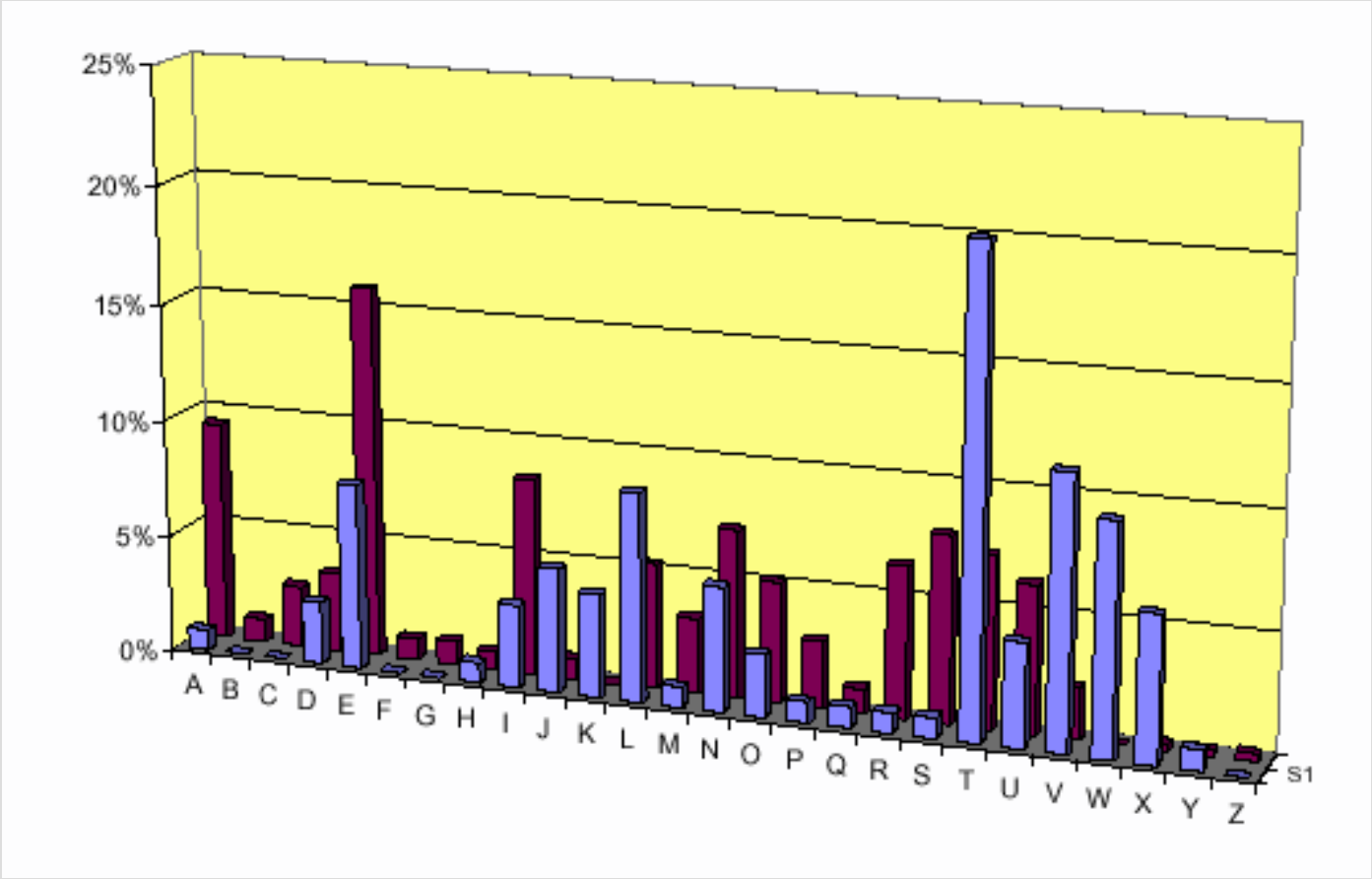
Cryptanalyse de la substitution mono alphabétique

Analyse des fréquences de caractères du texte chiffré



Cryptanalyse de la substitution mono alphabétique

Comparaison des fréquences entre texte clair et chiffré



Cryptanalyse de la substitution mono alphabétique

Début du déchiffrement

JeVMNKKeVLDE*VV*eLWeWIeKeXUeLWJ
ERUeVeWeHDXAeLIUNEWV.
JeVIEVWELOWENL*VV*NOEDJeVLePeXYe
LWeWUeSNLIeeVQXeVXUJXWEJEWeON
KKXLe.

Cryptanalyse de la substitution mono alphabétique

Suite du déchiffrement

lesMNKKesLDEsseLtetIeKeureLtlERreseteH
DuAeLIrNEts.
lesIEstELOtENLssNOEDlesLePeuYeLtetreS
NLIeesQuesurlutElEteONKKuLe.

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
				T							J	K	L				U	V	W	X	Y	Z	A	B	C

Cryptanalyse de la substitution mono alphabétique

Poursuite du déchiffrement

lesMNKKesLDEsseLtetIeKeureLtlERreseteH
DuAeLIrNEts.
lesIEstELOtENLssNOEDlesLePeuYeLtetreS
NLIeesQuesurlutElEteONKKuLe.

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
				T							J	K	L				U	V	W	X	Y	Z	A	B	C

Cryptanalyse de la substitution mono alphabétique

Poursuite du déchiffrement

les MNmmes nDEssent et Iemeurent
lERres et eHDux en IrNEts.
Les IEstEnOtENns sNOEDles ne Peuvent etre
SNLIees Que sur lutElEte ONmmune.

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
				T							J	K	L				U	V	W	X	Y	Z	A	B	C

Cryptanalyse de la substitution mono alphabétique

Fin du déchiffrement

« Les hommes naissent et demeurent
libres et égaux en droits.
Les distinctions sociales ne peuvent être
fondées que sur l'utilité commune. »

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

La substitution mono alphabétique

Les limites

Sur des textes donnant des fréquences très éloignées de celles habituelles :
De Zanzibar à la Zambie et au Zaïre, des zones d ’ozone font courir les zèbres en zigzags zinzins.

Une lettre / un digramme est toujours chiffré(e) de la même manière .

Idée d'amélioration :
– faire évoluer l'alphabet chiffré en cours de chiffrement !

—› Substitution **polyalphabétique** : utilisation de deux ou plus alphabets de chiffrement.

Exemple :

Alphabet clair : abcdefghijklmnopqrstuvwxyz
Alphabet chiffré 1: MOTSECRUVWXYZABDFGHIJKLNPQ
Alphabet chiffré 2: QPNLKJIHGFDBAZYXWVURCESTOM
Texte clair :
vinum et musica laetificant cor
Texte chiffré :
KGACZ KI AJUVNM BMKIGCGTQAR TYG

Chiffrement par substitution polyalphabétique

Le chiffre de Vigenère

- Le carré de Vigenère :
  26 alphabets : chiffrement de César
- Clé de chiffrement : un mot clé identifiant les alphabets à utiliser

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

Chiffre de Vigenère

Chiffrement

- Choix du mot-clé : *key*.
- Alphabets de chiffrement :

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

- Chiffrement d'un message :

m	e	n	s	s	a	n	a	i	n	c	o	r	p	o	r	e	s	a	n	o
K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y
W	I	L	C	W	Y	X	I	G	X	G	M	B	T	M	B	I	Q	K	R	M

Cryptanalyse de la substitution polyalphabétique

Deux étapes

- trouver la longueur du mot-clé ;
- faire l'analyse fréquentielle sur chacun des alphabets

Faiblesse

Taille de la clé : le codage d'un mot peut être le même, en particulier celui d'un digramme.

Il est possible de faire une **analyse fréquentielle** afin de déterminer la taille de la clé.

e	t	e	t	e	t	e	t
K	E	Y	K	E	Y	K	E
O	X	C	D	I	R	O	X

h	i	v	e	r	h	i	v	e	r	h	i	v	e	r	h	i	v	e	r
K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E	Y	K	E
R	M	T	O	V	F	S	Z	C	B	L	G	F	I	P	R	M	T	O	V

Cryptanalyse de la substitution polyalphabétiqe

NLPKMVGNSOXYPTGCEMQYHGDTGY
WGPWGEHGDSRTRKZRUPWVFRFPWFC
SKEWNPWRWYUAVGNMGFBFPPJZQOP
XQFXETXQJIPAIWEHQYGRLVNPVGNV
KCIKXTTTQGCPKMVGXIPEWCFJCCIRZ
RFCIFPPCMYUOIEPXVPPKMITEIFLRUW
IUNEUOIVPVOTRGDTCCPCWSK.

Cryptanalyse de la substitution polyalphabétiqe

Recherche de la longueur de la clé

On recherche des séquences qui se répétent de deux ou trois lettres et le nombre de caratères qui séparent ces répétitions :

NLPKMVGNSOXYPTGCEMQYHGDTGY
WGPWGEHGDSRTRKZRUPWVFRFPWFC
SKEWNPWRWYUAVGNMGFBFPPJZQOP
XQFXETXQJIPAIWEHQYGRLVNPVGNV
KCIKXTTTQGCPKMVGXIPEWCFJCCIRZ
RFCIFPPCMYUOIEPXVPPKMITEIFLRUW
IUNEUOIVPVOTRGDTCCPCWSK.

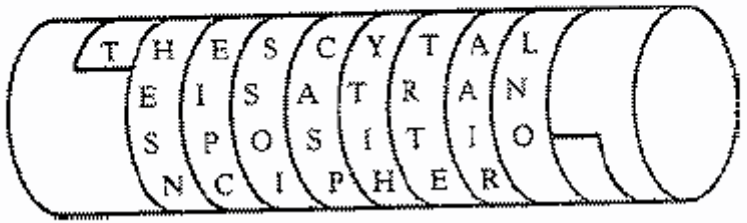
Séquence	Espace	Facteurs premiers
HGD	12	2 – 3
PW	6	2 – 3
	9	3
FP	24	2 – 3

Chiffrement par transposition

Toutes les lettres du message sont présentes, mais dans un ordre différent.
C'est un chiffrement de type *anagramme.*

Il utilise le principe mathématique des **permutations** (par colonne par exemple).

La *scytale* spartiate (5ème siècle av. JC) :



LA TRANSPOSTION PERMET EN THEORIE D'AVOIR UN HAUT DEGRE DE SECURITE

L	R	S	S	I	P	M	E	H	R	D	O	U	A	D	R	E	C	I
A	A	P	I	O	E	E	N	E	I	A	I	N	U	E	E	S	U	T
T	N	O	T	N	R	T	T	O	E	V	R	H	T	G	D	E	R	E

LRSSIPMEHRDOUADRECIAAPIOEENEIAINUEESUTTNOTNRTTOEVRHTGDERE

Chiffrement par transposition

Le chiffrement par transposition

Les méthodes de chiffrement par transposition consistent à **réarranger** les données à chiffrer de telle façon à les rendre **incompréhensibles**.

En général : **réarranger géométriquement** les données pour les rendre **visuellement** inexploitables.

Par exemple : "Ceci est un texte à chiffrer de la plus haute importance"

```
Ceci est un texte à chiffrer de la plus haute importance
```

Le texte est regroupé en tableau, suivant un nombre de colonnes donné.

```
Ceci est u
n texte à
chiffrer d
e la plus
haute impo
rtance
```

```
Cncehre h atctiluaiefatn…
```

Chaque colonne est ensuite copiée l'une après l'autre.

Cryptanalyse du chiffrement par tranposition

Cryptanalyse

- Déterminer si une substitution n'a pas été utilisée :
  une **analyse statistique** des caractères suffit à déterminer si les caractères ont été substitués (statistiques fréquentielles du texte identiques à celle d'un texte en clair).

- Si ce n'est pas le cas, il y a une **forte probabilité** pour qu'un chiffrement par **transposition** ait été employé.

- Ensuite, il faut faire une **hypothèse** sur le **nombre** de **colonnes** utilisées pour réaliser la transposition.

*Les codes de transposition contrairement aux codes par substitution **ne cachent pas** les caractères, mais modifient l'ordre des caractères*.

Et l'ordinateur fut…

L'arrivée des ordinateurs a totalement démodé ces méthodes de chiffrement *(on ne parle plus d'ailleurs de chiffrement car ces méthodes ne résiste pas au traitement informatique).*

La machine **Enigma** utilisée par les nazis a été « cassée » par Alan Turing, pionnier de l'informatique.

Il faut attendre les annés 60 pour voir les méthodes de **chiffrement moderne** basées sur l'usage de **clés**.

Comment renforcer la force des chiffrements ?

Combiner Substitution et Transposition

il est possible de faire subir aux caractères du « texte en clair » :

- une substitution ;
- plusieurs opérations de transposition.

Changer les paramètres de ces combinaisons très souvent

l'utilisation des paramètres de chaque opération doit être réduite au chiffrement de quelques messages avant d'être changés pour de nouveaux paramètres.

Combiner les paramètres

Les opérations sont connues, la séquence d'application des opérations est définie par la séquence des paramètres de chaque opération.

La combinaison des différents paramètres des différentes opérations permet de définir un **secret**.

Ce secret permet de réaliser le déchiffement et assure la sécurité du cryptogramme.
Il est appelé **clé de chiffrement**.

Le but

rendre l'apparence du cryptogramme la plus « aléatoire » possible, c-à-d. **éliminer les relations statistiques** des caractères du cryptogramme pour éviter la cryptanalyse :

Transposition + Substitution = Diffusion

L'actualité ?

les chiffrements tels que **DES** (*Data Encryption System*) et **AES** (*Advanced Encryption System*) sont utilisés à l'heure actuelle.

Le principe de Kerckhoffs

Auguste Kerckhoffs écrit en 1883 dans le *Journal des sciences militaires* un article intitulé « La cryptographie militaire » :

Il faut bien distinguer entre :
- un **système d'écriture chiffrée**, imaginé pour un échange momentané de lettres entre quelques personnes isolées ;
- une **méthode de cryptographie** destinée à régler pour un temps illimité la correspondance des différents chefs d'armée entre eux.

*Ceux-ci, en effet, ne peuvent, à leur gré et à un moment donné, **modifier leurs conventions**;*
*de plus, ils ne doivent jamais **garder sur eux aucun objet** ou **écrit** qui soit de nature à éclairer l'ennemi sur le sens des dépêches secrètes qui pourraient tomber entre ses mains.*

Premier cas : un grand nombre de combinaisons ingénieuses peuvent répondre au but qu'on veut atteindre ;
Second cas : il faut un système remplissant certaines **conditions exceptionnelles**, conditions que je résumerai sous les six chefs suivants:

- le système doit être **matériellement**, sinon **mathématiquement**, indéchiffrable ;
- Il faut qu'il **n'exige pas le secret**, et qu'il puisse sans inconvénient tomber entre les mains de l'ennemi;
- la **clé** doit **pouvoir** en **être communiquée** et retenue sans le secours de notes écrites, et être **changée** ou **modifiée** au gré des correspondants ;
- …

La notion de codage de l'information - Généralisation du codage

Et tout devint binaire…

La représentation informatique de document faite à base d'octets :

- au travers d'un **code standardisé** comme le code ASCII;
- directement comme la **couleur** d'un pixel d'une image ou bien **l'amplitude** d'un signal sonore, ou encore le code **d'instructions processeur** d'un logiciel,

a permis de généraliser les méthodes de cryptages à **tout type** de document.

Le message peut se traiter comme une **série d'octets**, voir **une suite** de **bits**, ou bien conserver son caractère initial (photo, texte, musique…).

La représentation des données

Unités de mesure

Le bit : unité de base qui prendre deux valeurs (0 ou 1)
contraction de « binary digit »

Bits : grouper en combinaison ils permettent d'exprimer un certain nombre de valeurs
Exemple avec 2 bits →

L'octet : groupe de 8 bits, byte en anglais
Il permet d'exprimer : 2 x 2 x 2 x 2 x 2 x 2 x 2 x 2 = 2^8 combinaisons possibles soient 256 valeurs.
Ces 256 valeurs suffisent à coder tous les caractères des langues européennes :
Exemple : J 01001010

Après normalisation par l'IEC « International Electrotechnical Commission »

Le kilo-octet	1 Ko	= 1000 octets	kibioctet (kio ou kiB) vaut 2^10 = 1024 octets
Le mega-octet	1 Mo	= 1000 Ko	Mébioctet (Mio ou MiB)vaut 2^20 =1 048 576 octets
Le giga-octet	1 Go	= 1000 Mo	Gibioctet (Gio ou GiB) vaut 2^30 =1 073 741 824 octets
			Tébioctet (Tio ou TiB) vaut 2^40 =1 099 511 627 776 octets

Symbole en anglais : kB pour kilo byte, kb pour kilo bit

Attention au valeurs annoncées par les constructeurs et les systèmes d'exploitation !

Codage de l'information

La table ASCII 7bits

Elle contient des caractères de contrôle pour les valeurs de 0 à 32.

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
0	00	Null	32	20	Space	64	40	@	96	60	`
1	01	Start of heading	33	21	!	65	41	A	97	61	a
2	02	Start of text	34	22	"	66	42	B	98	62	b
3	03	End of text	35	23	#	67	43	C	99	63	c
4	04	End of transmit	36	24	$	68	44	D	100	64	d
5	05	Enquiry	37	25	%	69	45	E	101	65	e
6	06	Acknowledge	38	26	&	70	46	F	102	66	f
7	07	Audible bell	39	27	'	71	47	G	103	67	g
8	08	Backspace	40	28	(	72	48	H	104	68	h
9	09	Horizontal tab	41	29	)	73	49	I	105	69	i
10	0A	Line feed	42	2A	*	74	4A	J	106	6A	j
11	0B	Vertical tab	43	2B	+	75	4B	K	107	6B	k
12	0C	Form feed	44	2C	,	76	4C	L	108	6C	l
13	0D	Carriage return	45	2D	-	77	4D	M	109	6D	m
14	0E	Shift out	46	2E	.	78	4E	N	110	6E	n
15	0F	Shift in	47	2F	/	79	4F	O	111	6F	o
16	10	Data link escape	48	30	0	80	50	P	112	70	p
17	11	Device control 1	49	31	1	81	51	Q	113	71	q
18	12	Device control 2	50	32	2	82	52	R	114	72	r
19	13	Device control 3	51	33	3	83	53	S	115	73	s
20	14	Device control 4	52	34	4	84	54	T	116	74	t
21	15	Neg. acknowledge	53	35	5	85	55	U	117	75	u
22	16	Synchronous idle	54	36	6	86	56	V	118	76	v
23	17	End trans. block	55	37	7	87	57	W	119	77	w
24	18	Cancel	56	38	8	88	58	X	120	78	x
25	19	End of medium	57	39	9	89	59	Y	121	79	y
26	1A	Substitution	58	3A	:	90	5A	Z	122	7A	z
27	1B	Escape	59	3B	;	91	5B	[	123	7B	{
28	1C	File separator	60	3C	<	92	5C	\	124	7C	|
29	1D	Group separator	61	3D	=	93	5D	]	125	7D	}
30	1E	Record separator	62	3E	>	94	5E	^	126	7E	~
31	1F	Unit separator	63	3F	?	95	5F	_	127	7F	□

Le codage de l'information

La table ASCII étendue sur 8 bits

Elle ajoute des caractères accentués et des caractères de dessin ou de formules.

Elle dépend du constructeur qui la définit.

Un exemple de table ASCII étendue

Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char	Dec	Hex	Char
128	80	Ç	160	A0	á	192	C0	└	224	E0	α
129	81	ü	161	A1	í	193	C1	┴	225	E1	ß
130	82	é	162	A2	ó	194	C2	┬	226	E2	Γ
131	83	â	163	A3	ú	195	C3	├	227	E3	π
132	84	ä	164	A4	ñ	196	C4	─	228	E4	∑
133	85	à	165	A5	Ñ	197	C5	┼	229	E5	σ
134	86	å	166	A6	ª	198	C6	╞	230	E6	µ
135	87	ç	167	A7	º	199	C7	╟	231	E7	τ
136	88	ê	168	A8	¿	200	C8	╚	232	E8	Φ
137	89	ë	169	A9	⌐	201	C9	╔	233	E9	Θ
138	8A	è	170	AA	¬	202	CA	╩	234	EA	Ω
139	8B	ï	171	AB	½	203	CB	╦	235	EB	δ
140	8C	î	172	AC	¼	204	CC	╠	236	EC	∞
141	8D	ì	173	AD	¡	205	CD	═	237	ED	ø
142	8E	Ä	174	AE	«	206	CE	╬	238	EE	ε
143	8F	Å	175	AF	»	207	CF	╧	239	EF	∩
144	90	É	176	B0	░	208	D0	╨	240	F0	≡
145	91	æ	177	B1	▒	209	D1	╤	241	F1	±
146	92	Æ	178	B2	▓	210	D2	╥	242	F2	≥
147	93	ô	179	B3	│	211	D3	╙	243	F3	≤
148	94	ö	180	B4	┤	212	D4	╘	244	F4	⌠
149	95	ò	181	B5	╡	213	D5	╒	245	F5	⌡
150	96	û	182	B6	╢	214	D6	╓	246	F6	÷
151	97	ù	183	B7	╖	215	D7	╫	247	F7	≈
152	98	ÿ	184	B8	╕	216	D8	╪	248	F8	°
153	99	Ö	185	B9	╣	217	D9	┘	249	F9	∙
154	9A	Ü	186	BA	║	218	DA	┌	250	FA	·
155	9B	¢	187	BB	╗	219	DB	█	251	FB	√
156	9C	£	188	BC	╝	220	DC	▄	252	FC	ⁿ
157	9D	¥	189	BD	╜	221	DD	▌	253	FD	²
158	9E	₧	190	BE	╛	222	DE	▐	254	FE	■
159	9F	ƒ	191	BF	┐	223	DF	▀	255	FF	

Le code ANSI « American National Standard Institute »

C'est une norme pour les caractères supplémentaires.

La table est associée à code pays.

Exemple : la page de code 850

Page de codes 850

		0	16	32	48	64	80	96	112	128	144	160	176	192	208	224	240
		0-	1-	2-	3-	4-	5-	6-	7-	8-	9-	A-	B-	C-	D-	E-	F-
0	-0		►		0	@	P	`	p	Ç	É	á	▒	└	ð	Ó	
1	-1	☺	◄	!	1	A	Q	a	q	ü	æ	í	▒	┴	Ð	ß	±
2	-2	☻	↕	"	2	B	R	b	r	é	Æ	ó	▓	┬	Ê	Ô	‗
3	-3	♥	!!	#	3	C	S	c	s	â	ô	ú	│	├	Ë	Ò	¾
4	-4	♦	¶	$	4	D	T	d	t	ä	ö	ñ	┤	─	È	õ	¶
5	-5	♣	§	%	5	E	U	e	u	à	ò	Ñ	Á	┼	ı	Õ	§
6	-6	♠	▬	&	6	F	V	f	v	å	û	ª	Â	ã	Í	µ	÷
7	-7	•	↨	'	7	G	W	g	w	ç	ù	º	À	Ã	Î	þ	¸
8	-8	◘	↑	(	8	H	X	h	x	ê	ÿ	¿	©	╚	Ï	Þ	°
9	-9	○	↓	)	9	I	Y	i	y	ë	Ö	®	╣	╔	┘	Ú	¨
10	-A	◙	→	*	:	J	Z	j	z	è	Ü	¬	║	╩	┌	Û	·
11	-B	♂	←	+	;	K	[	k	{	ï	ø	½	╗	╦	█	Ù	¹
12	-C	♀	∟	,	<	L	\	l	|	î	£	¼	╝	╠	▄	ý	³
13	-D	♪	↔	-	=	M	]	m	}	ì	Ø	¡	¢	═	¦	Ý	²
14	-E	♫	▲	.	>	N	^	n	~	Ä	×	«	¥	╬	Ì	¯	■
15	-F	☼	▼	/	?	O	_	o	⌂	Å	ƒ	»	┐	¤	▀	´	

La stéganographie ou l'art de la dissimulation

En grec :

Stéganographie : (στεγανο γραφ ην)

écriture couverte . Connaissance de l'existence de l'information —› Connaissance de l'information

Cette méthode consiste à **dissimuler l'information** à chiffrer dans une autre information.
On appelle cette méthode la «stéganographie».
Exemple : utiliser un bit tous les 8 bits dans une image (un bit de poids faible de préférence).
L'image est faiblement modifiée et rien ne permet de savoir qu'elle contient un message caché.

Cette méthode peut être utilisé en plus de techniques de cryptographie avancée et permet d'en dissimuler l'usage.

Elles peut être utilisées de manières différentes :

- en associant un **groupe de lettres** à un **caractère** et en composant un texte qui ait un sens pour les groupes de lettres, par exemple dans un compte rendu de partie d'échec où chaque coup joué correspond à une lettre du message secret et donne l'illusion d'une partie « normale »;
- le filigrane ou “**watermarking**” pour dissimuler une information dans un document pour en permettre l'identification (protection des droits d'auteur);
- le **canal de communication caché** ou “cover channel” qui permet de diposer d'un véritable canal de communication en détournant l'usage de canaux de communications anodins. Cette technique permet de déjouer l'usage de firewall.
  Exemple : ralentir artificiellement un transfert ftp ou au contraire l'accélérer pour coder un bit à 1 ou à 0, et pouvoir transmettre à un observateur le message qu'il construit.

La cryptanalyse reste **difficile** et doit s'appliquer à de **gros volumes** de données à **l'aveugle**.

La notion d'original et de copie

Notion de copie et d'original d'un document papier

Une photocopie est différente de l'original (*ou presque…*).
Essayez de présenter la photocopie d'un billet pour acheter dans une boutique !

Une personne est identifiée par sa signature (analyse graphologique)
Cette signature engage la personne qui l'a écrite :

- c'est une preuve **d'acceptation** pour un contrat et **d'engagement** à le remplir ;
- c'est une **autorisation** de transfert d'argent dans le cas d'un chèque ;
- c'est une **identification** dans le cas d'une lettre que l'on envoie.

Cette signature est reconnue par la législation française.

Notion de copie « **certifiée conforme**» réalisable auprès de la mairie ou bien d'un commissariat.
Cette notion a d'ailleurs disparue, face à l'avancée des moyens de reproduction et de l'utilisation systématique de l'impression machine pour les documents administratifs (plus ou presque de partie manuscrite présente sur le document ou bien reproduite électroniquement).

Signature

Une signature manuscrité idéale est réputée posséder les propriétés suivantes :

- Elle ne peut être imitée ;
- Elle **authentifie** le signataire ;
- La signature appartient à un seul document (elle n'est pas réutilisable) ;
- Le document ne peut être partiellement ou totalement modifié ;
- La signature ne peut être **reniée** ;
- La signature peut être **contrôlée**.

Copie ou original

Le cas du document électronique

Il est **reproductible** à l'infini sans modification.
C'est ce qui le rend virtuellement éternel.

Le droit de copie, dite de sauvegarde, est apparu avec l'apparition de « programme informatique » sur support duplicable (bande magnétique, disquette, CD…).

Il peut être **modifié** pour faire **disparaitre** ou **apparaitre** des éléments supplémentaires.
Suppression du nom de l'auteur d'un document de traitement de texte, ajout d'un texte de propriété sur une image…

Il peut être **attribuer** à n'importe quel propriétaire.
Un fichier MP3 peut appartenir à une personne disposant du CD qui a servi de source à son encodage ou bien à une autre…

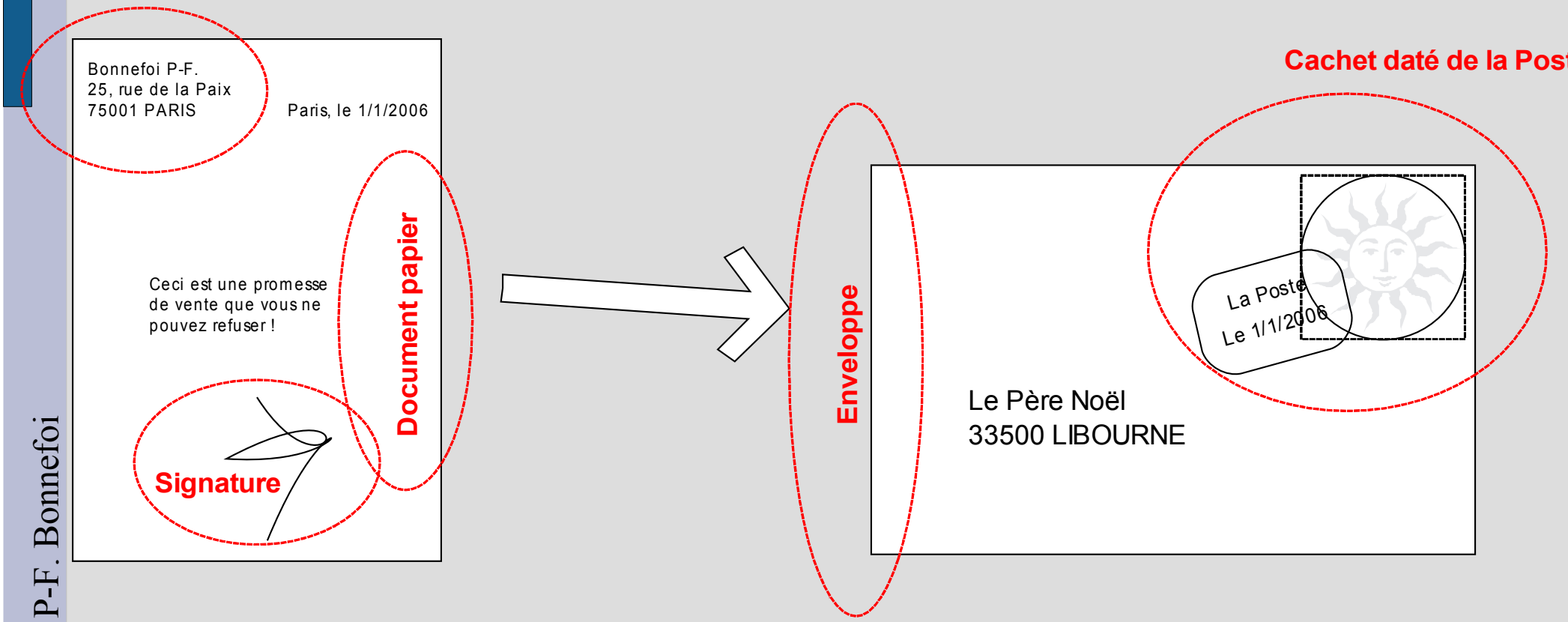
Une **nouvelle forme** de **propriété** est apparue avec lui : celle liée à la **consultation** du contenu sans possibilité d'exploitation ou de reproduction en vu de conservation.

C'est le cas du DVD dont le contenu ne peut (ne pouvait) être accéder que pour le visionner mais pas pour l'enregistrer ou le modifier.

La sécurité « écrite » : la signature et l'envoi par la Poste

Pour être recevable comme document engageant la responsabilité de celui qui l'envoi le document doit possèder :

- une indication claire de **l'identité** ;
- une **signature** ;
- *ces deux indications doivent être apposés sur un même papier (pas de collage, ...) ;*
- mis dans une **enveloppe** avec le **cachet** de la Poste.



La sécurité « électronique » : la signature électronique

Vers la signature électronique : des considérations juridiques

Les régimes juridiques doivent admettre les écrits numériques comme :

- **recevables** (*le juge a le droit de les considérer*) ;
- potentiellements **probants** (*ils apportent la preuve s'ils sont difficilement falsifiable*).

Les travaux de normalisation se concentrent sur deux aspects :

- **l'interopérabilité** pour une signature électronique universellement interprétée et reconnue
  définition de **standards d'interprétation non ambigüe des signatures ;**
  des algorithmes de calcul et des modes de fonctionnement ;
  des initiatives privées (RSA Security Inc) ont déja établi des formats de messages;

- **la sécurité** ;
  la norme internationale des "**critères communs**" de **spécification** et **d'évaluation sécuritaire** ouvre la perspective de la reconnaissance des signatures entre pays par le fait que leurs niveaux de sécurité soient équivalents.

La vérification des **caractèristiques de sécurité** des **systèmes** est effectuées par des **sociétés spécialisées**, les *évaluateurs*; dont les compétences sont surveillées entre autres, par une autorité émanant de l'état la **DCSSI**.

Le **risque zéro** n'existe pas et **l'arsenal juridique** et technique doit **prendre** en **compte** ce fait, en prévoyant les **conséquences d'accidents majeurs** (fraudes ou dysfonctionnement) dans des plans de secours.

La signature électronique : aspects juridiques

Le 13 décembre 1999, de la directive 1999/93/CE relative à "un cadre communautaire pour les signatures électroniques"

La loi du 13 mars 2000

Au contraire de la directive, la loi française ne rentre dans aucune considération technique.

Elle définit de façon générale la signature, au regard des fonctions assurées par celle-ci : "*La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte*" (art. 1316-4 du Code Civil).

Le code civil définit également les conditions de l'équivalence du support électronique et du support papier à titre de preuve, sous réserve que quatre conditions soient respectées : Les quatre conditions posées par le code civil pour que le support numérique soit admissible comme preuve au même titre que le support papier

1 - **pouvoir identifier** la personne dont émane l'écrit électronique au moyen d'un procédé fiable ;

2 - l'écrit électronique a été **créé** dans des conditions de nature à en **garantir l'intégrité** ;

3 - l'écrit électronique est **conservé** dans des conditions de nature à en **garantir l'intégrité**

4 - utiliser un procédé fiable **garantissant** le **lien** de la **signature électronique** avec **l'acte** auquel elle s'attache.

Le décret du 30 mars 2001

Le décret est un texte technique, qui constitue la transposition de la **directive européenne** sur la signature électronique.

Il distingue la « signature électronique » de la « signature électronique sécurisée » :

- la **signature électronique** est celle qui respecte les conditions posées par le code civil ;
- la **signature électronique sécurisée** est celle qui répond de plus aux exigences du décret, et présente de ce fait une présomption de fiabilité.

Le décret précise les conditions de mise en oeuvre de la "signature électronique sécurisée", qui bénéficie d'une présomption de fiabilité :

- elle est établie grâce à un dispositif sécurisé de création de signature électronique ;
- sa vérification repose sur l'utilisation d'un **certificat électronique qualifié**.

Le secret de la correspondance

Il y a violation de secret de la correspondance lorsqu'une tierce personne en prend connaissance sans le consentement préalable de l'émetteur d'un courrier à caractère privé ou en dehors du cadre de la Loi.

Une correspondance reste la **propriété intellectuelle** de son auteur bien que le support physique soit la propriété du destinataire.

La convention européenne de sauvegarde des droits de l'Homme et des libertés fondamentales du 4 novembre 1950, rappelle en son article 8, "*le droit au respect de la correspondance*".

Union européenne

Au sein de l'Union européenne, le secret de la correspondance est garanti par la **directive européenne 97/66 du 15 décembre 1997** qui fait obligation aux États-membres de garantir par leur législation :

- la confidentialité des communications passées par la voie des télécommunications et d'interdire "à toute autre personne que les utilisateurs, sans le consentement des utilisateurs concernés, d'écouter, d'intercepter, de stocker les communications ou de les soumettre à quelque autre moyen d'interception ou de surveillance, sauf lorsque ces activités sont légalement autorisées. "

France

En France, la **violation de secret** de la correspondance est actuellement réprimée par les articles 226-15 et 432-9 du code pénal et par l'article L 33-1 du code des postes et télécommunications.

L'e-administration

Le ministre délégué au Budget et à la Réforme de l'État, Jean-Francois Copé, a présenté un projet de loi ratifiant l'ordonnance du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives, et entre les autorités administratives elles-mêmes.

Cette ordonnance, prise sur le fondement de la loi du 9 décembre 2004, de simplification du droit, vient renforcer l'attirail juridique nécessaire au bon développement de "l'administration électronique" dans le pays.

L'e-administration

Elle concerne

- l'ensemble des **échanges électroniques** ;
- télé-services ou courriels échangés avec les administrations, qu'il s'agisse des administrations de l'État, des collectivités territoriales, de leurs établissements publics administratifs, des organismes de sécurité sociale ou des autres organismes de droit privé gérant des services publics administratifs.

L'ordonnance a établi une **équivalence juridique** entre le **courrier électronique** et le **courrier** sur **support papier** en prévoyant notamment que la *saisine de l'administration par voie électronique est régulière* et doit faire l'objet d'un *accusé de réception* ou d'un accusé d'enregistrement informant l'usager que sa demande a été prise en compte.

Elle offre ainsi la possibilité aux usagers de disposer d'un **espace de stockage** en ligne, personnalisé et personnalisable, qui a pour vocation d'accueillir les documents administratifs les concernant, ainsi qu'un bloc-notes contenant des formulaires en ligne.

Ce service sera expérimenté début 2006 avant sa mise en place en 2007. Le texte permet également la mise place des conditions permettant la **signature électronique** de leurs actes par les autorités administratives.

Échange sur Internet

Transmission du document par réseau

La transmission d'un document numérique (exemple un CD) peut se faire par la Poste avec accusé de réception et pli cacheté, la sécurité est celle offerte par la Poste.

Mais, elle est de plus en plus liée à **l'utilisation** de **réseaux**, ce qui l' expose à des problèmes nouveaux:

- le document peut être **intercepté**, **falsifié**, **abimé** ;
- qui est réellement **l'expéditeur** du document ;
- qui à le droit à la **réception** de déchiffrer son sontenu ;
- quand a-t-il été transmis et a-t-il été déja transmis précédemment.

Les risques liés aux réseaux

Il **n'existe pas** de réseau dans lequel les transmissions ne peuvent être **observées**.

Les informations qui transitent peuvent toujours être **récupérées**.

Il existe des protections **physiques** ponctuelles :

- câble **blindé enfermé** dans un tube contenant un **gaz** inerte; si quelqu'un essaye de se connecter sur le câble (utilisation d'une connexion vampire) le tube est percé et le gaz s'échappe. Il suffit de vérifier la pression du gaz dans le tube pour s'assurer qu'il n'y a pas eu d'intrusion.
- **fibre optique**; les caractéristiques des fibres optiques permettent de savoir s'il y a eut rupture.

Ces protections sont **inefficaces**, quand les paquets de données doivent transiter par un **routeur**.

L'utilisation de «garde-barrière» ou “**firewall**” permet d'éviter à des paquets :

- de transiter par des réseaux vulnérables;
- de sortir d'un réseau protéger.

Échange sur Internet

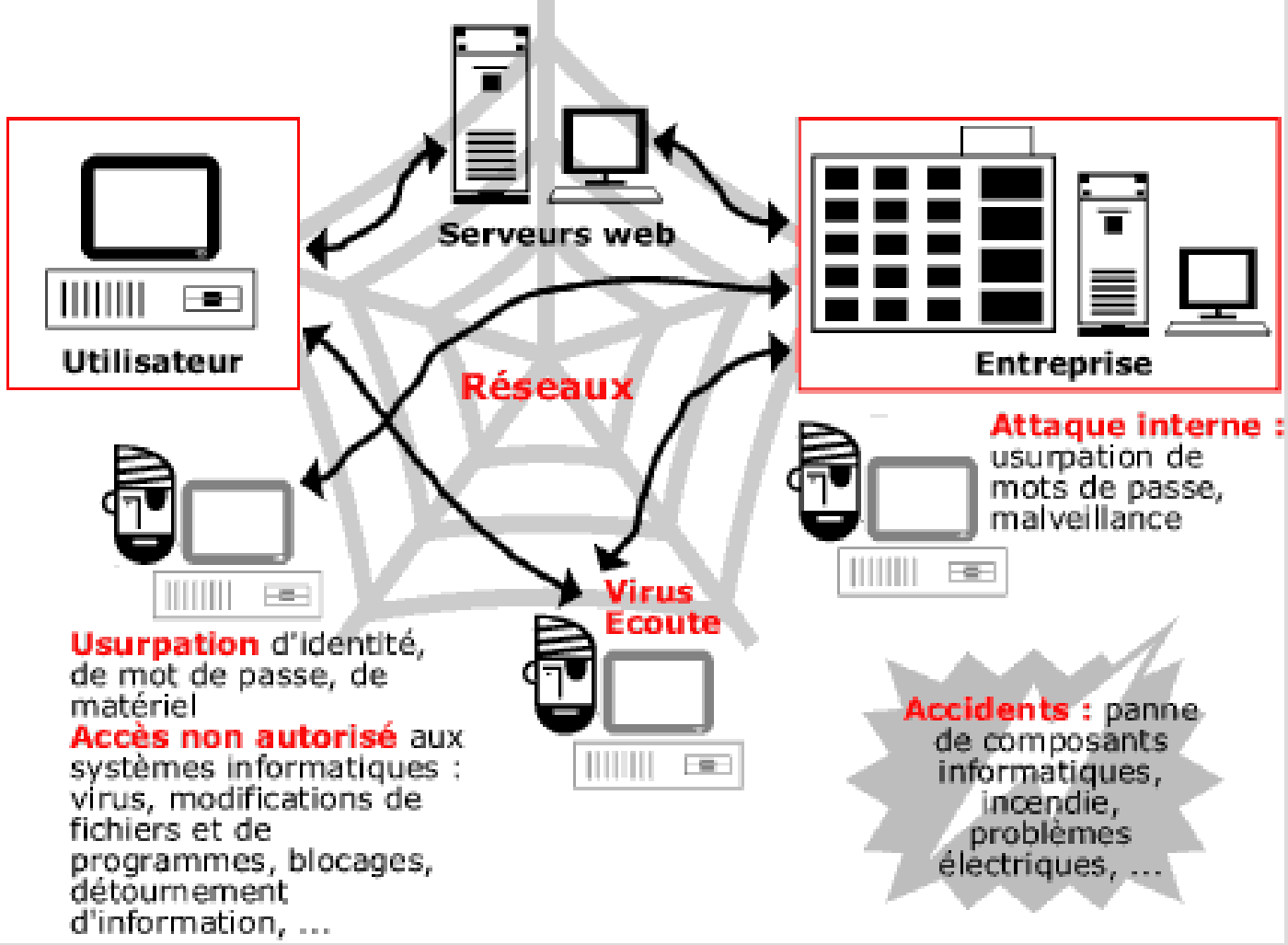
Les besoins en sécurité liés au réseau

Les réseaux sont de plus en plus utilisés pour effectuer des opérations bancaires ou des achats par correspondance.

Il s'agit d'empêcher :

- **l'interception** des messages : mot de passe, courrier électroniques…
- **l'intrusion** des Systèmes : vol de données, mise en place de virus, destruction d'information, détournement de biens…
- la **fraude** : faux client, vendeur escroc…

Les dangers que courent un système informatique



Les domaines où peut intervenir la cryptographie

Authentification (détermination de l'identité de l'interlocuteur)
Le serveur est-il réellement celui qu'il dit être? L'utilisateur est-il bien celui qu'il prétend être?
Usurpation d'identité

Intégrité (l'assurance que l'information stockée ou transmise n'est pas altérée)
L'information reçue est-elle identique à celle émise? Mes fichiers sont-ils corrompus? L'information est-elle fiable?
Modification accidentelle ou intentionnelle de l'information hébergée ou des transactions électroniques

Confidentialité (la connaissance de l'information par un groupe restreint de personnes ou de systèmes)
L'information n'est-elle connue que de l'émetteur et du récepteur? L'information stockée est-elle accessible uniquement aux personnes autorisées?
Détournement de l'information, appropriation non autorisée d'informations

Autorisation (la permission de faire ou d'accéder à quelque chose)
Qui peut accéder à mon ordinateur pendant mon absence? L'utilisateur distant accède-t-il uniquement aux services et informations pour lesquels il a obtenu une autorisation?
Accès non autorisé à des ressources ou informations

Non répudiation (protection contre la négation d'une action accomplie)
Le fournisseur de services peut-il faussement prétendre qu'il n'a pas reçu ou effectué la transaction? L'utilisateur peut-il faussement prétendre qu'il n'a pas effectué une transaction?
Nier avoir passé une commande électronique ou avoir effectué un achat

Sécurité informatique

Traçabilité (garder un historique des événements**)**
Qui a fait quoi, utilisé quoi et quand?
Impossibilité de reconstituer les étapes qui ont conduit à un incident

Intrusion (accès non autorisé)
Comment protéger mon système personnel? Comment détecter les intrus? Comment protéger le serveur?
Accès non autorisés et actions malveillantes (introduction de virus ou de mouchards, modification de contenu, blocage des accès,..), accès non souhaités (e-mail publicitaire)

Protection physique (protection contre les accidents ou sabotage)
Garder l'intégrité des informations en cas de panne de courant, dégâts des eaux, incendie, ...
Interruption non prévue de l'opérationnel et impossibilité de redémarrage rapide, dégâts irréversibles du matériel, de données

Gestion des procédures, des ressources humaines et machines
Que doit-on faire? Qui fait quoi, qui est responsable de quoi, qui met à jour quoi? Qui peut entrer en salle machine?
Pas de contrôle, manque de rigueur dans la gestion des mots de passe, des mises à jour des fichiers d'autorisation d'accès, des fichiers d'audit, de la configuration des routers et firewalls, ...

Cryptographie moderne - Le cryptage à clé

Cryptographie moderne

Ce type de chiffrement repose sur l'utilisation :

- d'un algorithme **public**, connu de tous;
- d'une **clé**.

Il correspond à la cryptographie moderne, par rapport aux codes par substitution et transposition.

Auparavent, les algorithmes étaient **simples** mais utilisaient des **clés longues**.
Exemple : un XOR entre le message à transmettre et une clé de même taille suffit à le rendre indéchiffrable…technique du masque jetable

Maintenant, le but est d'utiliser des algorithmes **sophistiqués** et **complexes** associés à des **clés courtes**.

Ces algorithmes représente des investissements à long terme, c-à-d. qu'ils sont employés pendant de nombreuses années jusqu'à ce qu'ils en puissent plus assurer le même niveau de sécurité.

Il existe **deux sortes** de cryptage :

- à clé **symétrique** ;
- à clé **asymétrique**.

Hypothèse de base de la cryptanalyse :
Principe de Kerckhoff -- Auguste Kerckhoff, ``La cryptographie militaire", février 1883

L'opposant connaît le système cryptographique
&
Toute la sécurité d'un système cryptographique doit reposer sur la clé, et pas sur le système lui-même

Chiffrement à clé symétrique

Principe

Le cryptage à clé symétrique (ou secrète)

La **même clé** doit être employée pour chiffrer ou déchiffrer le message;

Le chiffrement consiste alors à effectuer une opération entre la clé privée et les données à chiffrer.

Le déchiffrement se fait à l'aide de cette **même clé secrète**.

Remarques

La qualité d'un crypto système symétrique se mesure par rapport :

- à des propriétés statistiques des textes chiffrés ;
- à la résistance aux classes **d'attaques connues**.

En pratique : *tant qu'un crypto système symétrique n'a pas été cassé, il est bon, après il est mauvais !*

Chiffrement à clé asymétrique

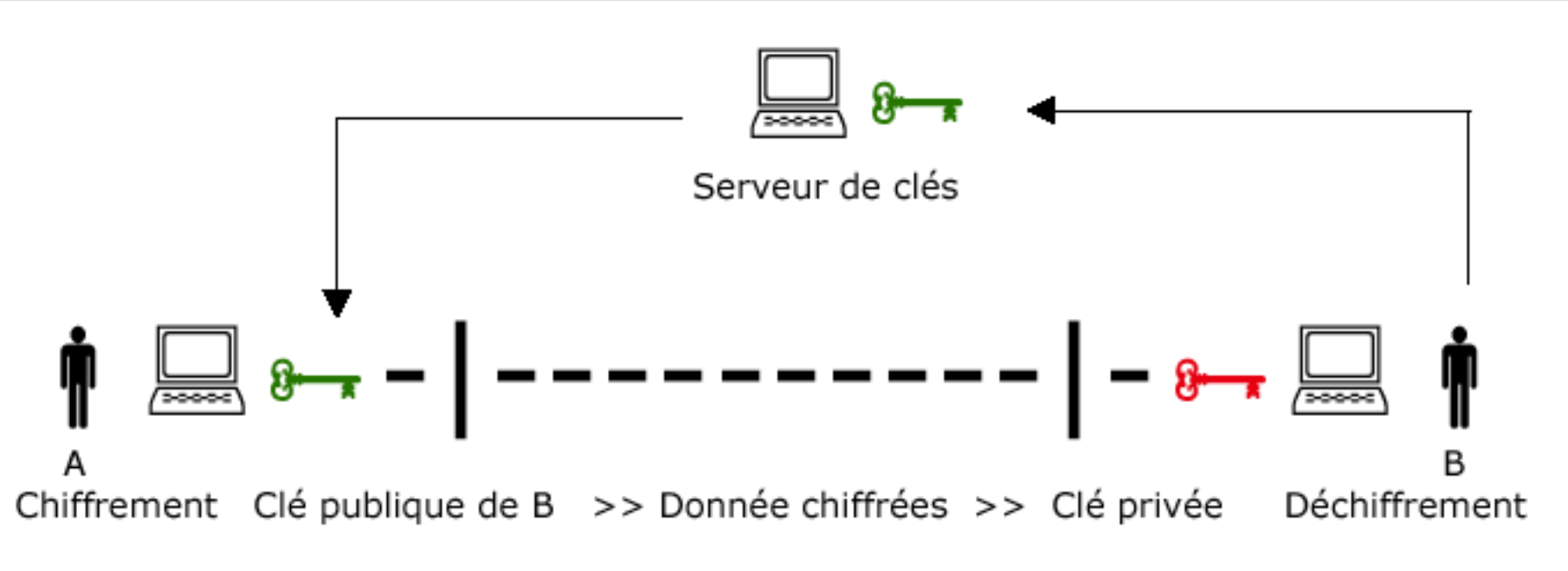
Principe

Il utilise :

- une **clé publique** connue de tous ;
- une **clé privée** connue seulement du destinataire du cryptogramme.

Ces chiffrements a « clé publique» ont été découvert par James Ellis (Angleterre) en 1969 et par Whitfield Diffie (Etats unis) en 1975.

L'idée de la conception de tels algorithmes revient à Diffie et Hellman en 1976.

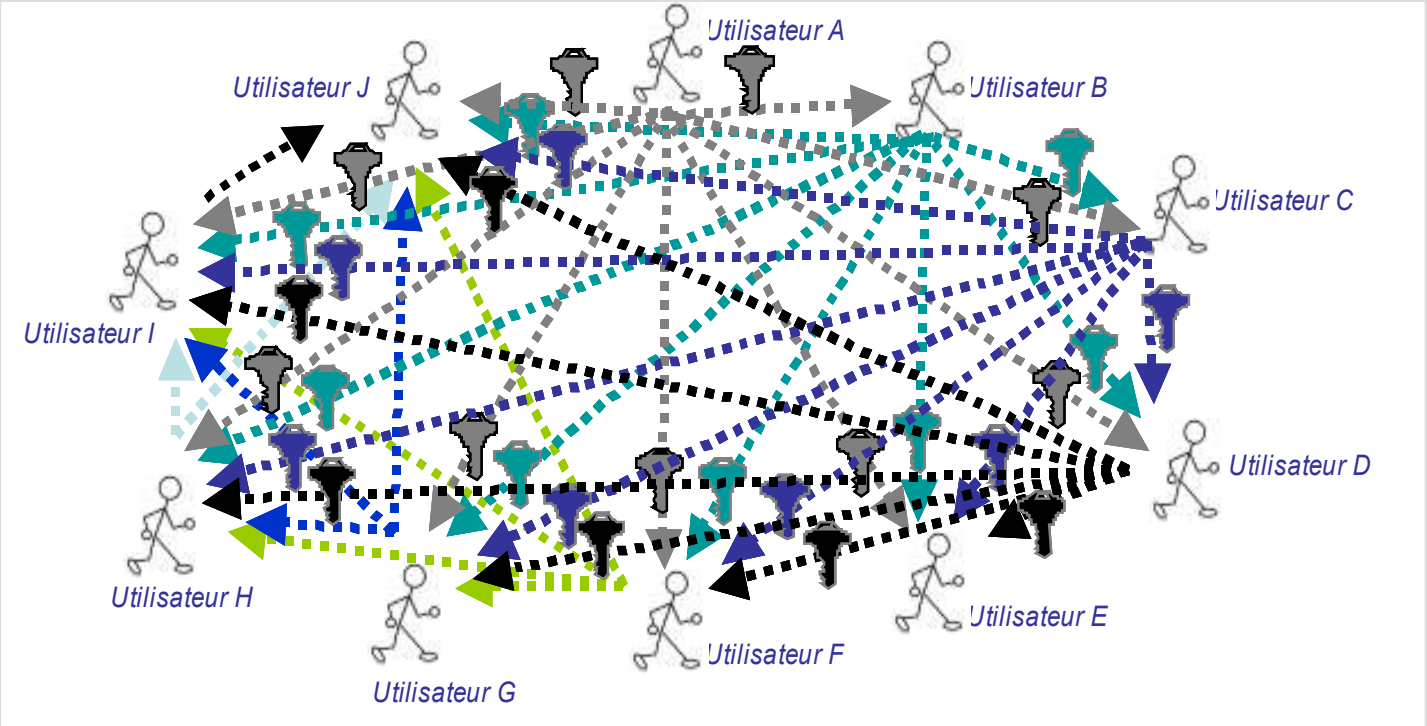


Les limites de la cryptographie Symétrique

La multiplication des clés

Pour établir un canal de communication entre deux individus :

- Il faut qu'il soit chiffré avec une **clé partagée** entre les deux individus ;
- Il est ainsi confidentiel pour ceux qui ne possède pas la clé de chiffrement.

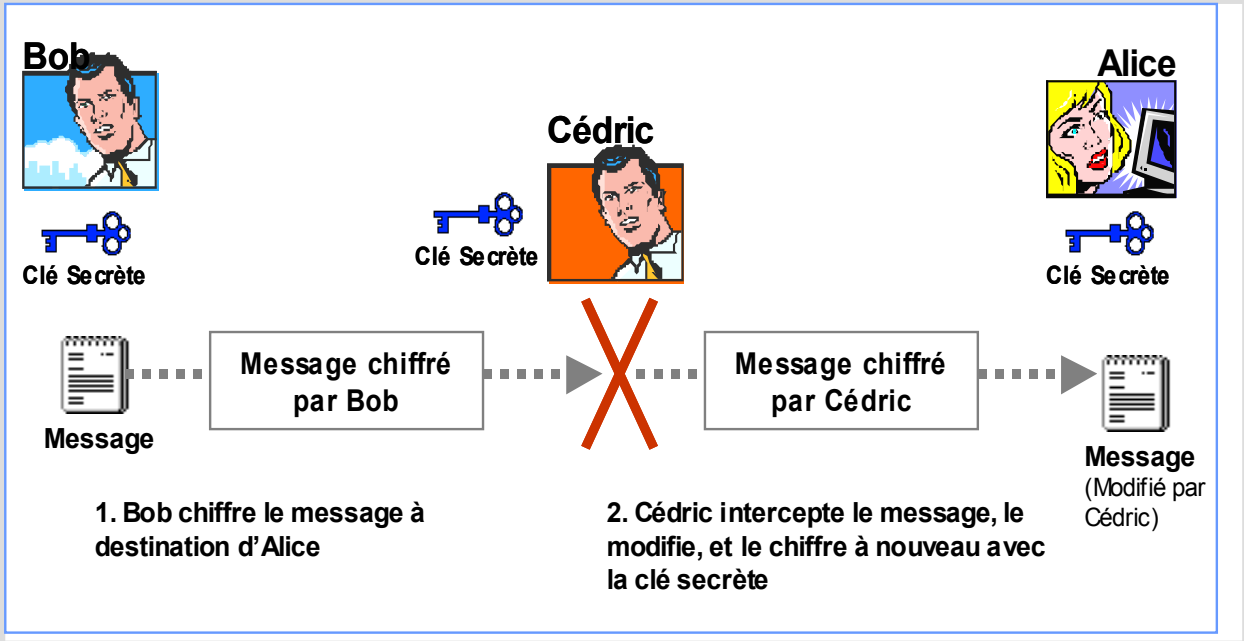


Pour que deux canaux de communications soient indépendants l'un de l'autre, c-à-d. qu'une personne accède à l'un mais pas à l'autre, il faut que ces deux canaux utilisent des clés différentes.
Il est possible qu'un des interlocuteurs connaissent plusieurs clés utilisés dans différents canaux le reliant à des utilisateurs différents.
Exemple : l'utilisateur D possède une clé pour chaque lien (avec J, I, H, G, F et E).
Problème : comment échanger toutes ces clés ?

Les limites de la cryptographie Symétrique

Pas d'intégrité et d'identification de l'auteur

Si Alice, Bob et Cédric partage le même lien de communication alors ils partagent la même clé de chiffrement symétrique.



Chacun peut intercepter et modifer les messages qui s'échangent.

Chiffrement asymétrique

Construction des clés

Les utilisateurs (A et B) choisissent une **clé aléatoire** dont ils sont seuls connaisseurs (il s'agit de la clé privée).

A partir de cette clé, ils **déduisent** chacun automatiquement par un algorithme la **clé publique**.
Les utilisateurs **s'échangent** cette clé publique au travers d'un canal **non sécurisé**.

Chiffrement d'un message

Lorsqu'un utilisateur désire **envoyer un message** à un autre utilisateur, il lui suffit de **chiffrer** le message à envoyer au moyen de la **clé publique** du destinataire (qu'il trouvera par exemple dans un serveur de clés tel qu'un annuaire ou bien en signature d'un courrier électroique).

Le destinataire sera en mesure de **déchiffrer** le message à l'aide de sa clé privée (**qu'il est seul** à **connaître**).

Rapports entre les clés

La recherche de la clé privée à partir de la clé publique revient à résoudre un **problème mathématique notoirement très compliqué**, c-à-d. demandant un **grand nombre d'opérations** et beaucoup de mémoire pour effectuer les calculs -> infaisable !

Par exemple dans RSA, l'algorithme le plus utilisé actuellement, la déduction de la clé privée à partir de la clé publique revient à résoudre un problème de factorisation de grand nombre que lequel travaille les mathématiciens depuis plus de 2000 ans !

Le choix des clés doit être fait de la manière la plus **imprédictible possible** : éviter les mots du dictionnaire, nombres **pseudo-aléatoires** à germe de génération difficile à deviner, etc.

Prise en en compte de la notion d'échange par réseau

Echange par réseau

L'objectif de la cryptographie est de permettre à deux personnes, **Alice** et **Bob**, de communiquer au travers d'un canal peu sûr (téléphone, réseau informatique ou autre), sans qu'un opposant,**Oscar**, puisse comprendre ce qui est échangé.

Alice souhaite transmettre à **Bob** un ensemble de données (texte, nombres, …).

Alice transforme ces informations par un procédé de chiffrement en utilisant une clé prédéterminée, puis envoie le texte chiffré au travers du canal de communication.

Oscar, qui espionne peut-être le canal, ne peut reconstituer l'information, contrairement à **Bob** qui dispose de la clé pour déchiffrer le cryptogramme.

Les éléments fondamentaux de la sécurité

Quatres besoins fondamentaux à satisfaire simultanément

Intégrité des données

Le contrôle d'intégrité d'une donnée consiste à vérifier que cette donnée n'a pas été modifiée, frauduleusement ou accidentellement.

Confidentialité

Il s'agit de rendre l'information inintelligible à tous les Oscar, aussi bien lors de sa conservation qu'au cours de son transfert par un canal de communication. L'information n'est consultable que par son destinataire uniquement.

Contrôle d'accès

Il s'agit d'authentifier les utilisateurs de façon à limiter l'accès aux données, serveurs et ressources par les seules personnes autorisées.

Identification/authentification

Le contrôle d'identification consiste à s'assurer que Bob est bien Bob (**authentification des partenaires**) et d'obtenir une garantie qu'Alice a bien déclenché l'action (**authentification de l'origine des informations**).
C'est un problème fondamental, qui exige de faire confiance à un tiers dans le cas où les deux interlocuteurs ne se connaissent pas au préalable.

Non-répudiation

Elle joue le rôle de **signature contractuelle**, c-à-d. qu'une personne ne peut revenir sur ce qu'elle a transmis. Il n'y a pas pu y avoir de transmission de sa part sans son accord.
Alice ne peut nier l'envoi d'information ; Bob ne peut nier la réception d'information ; ni l'un ni l'autre ne peuvent nier le contenu de cette information (très important lors du passage d'une commande par exemple).
Une personne ne peut prendre l'identité d'une autre pour transmettre une information en son nom.

Une approche théorique

Cryptage à clé symétrique

Ce cryptage repose sur la définition d'une formule mathématique de la forme :

Donnée chiffrées = Fonction (données, clé)

Avec une fonction inverse de la forme :

Données = Fonction_inverse (données_chiffrées, clé)

Dans cette méthode de chiffrement, on distingue deux types d'algorithmes :

- l'algorithme **par bloc** qui prend une longueur spécifiée de données comme entrée, et produit une longueur différente de données chiffrées (exemple : DES, AES…)
- l'algorithme en **flux continu** qui chiffre les données un bit à la fois (exemple : IDEA, CAST, RC4, SKIPjack…).

Avantages et inconvénients d'un cryptosystème à clé symétrique

Le principal inconvénient d'un cryptosystème à clefs secrètes provient de **l'échange** des **clés**.
Le chiffrement symétrique repose sur **l'échange d'un secret** (les clés).

Pour être totalement sûr : les chiffrements à clés secrètes doivent utiliser des clés d'une longueur au moins égale à celle du message à chiffrer (*One Time Pad ou « Masque Jetable »*)
En pratique : les clés ont une taille donnée, **suffisante**.

Lors d'échange entre **plusieurs intervenants** : une clé est partagée que par 2 interlocuteurs, donc pour N interlocuteurs il faut N*(N-1)/2 clés.

Aproche théorique & Chiffrement symétrique

La plupart des codes utilisés
- sont **relativements rapides** ;
- peuvent s'appliquer à un **fort débit** de donnée à transmettre.

Il existe des processeurs spécialement conçu pour réaliser le chiffrement et le déchiffrement.

Principaux algorithmes utilisés :
- DES, *Data Encryption System* IBM 1977 ;
- IDEA, *International Data Encryption Algorithm* Lai et Massey 1990 ;
- Blowfish, Schneir 1994.

Problème d'assurer la sécurité des clés.

Problème de la **distribution des clés**, qui doit se faire par un canal qui doit être sûr.

La valise diplomatique dans le cas du téléphone rouge…

Chiffrement asymétrique

Cryptage à clé asymétrique

Il repose sur la connaissance d'une fonction mathématique **unidirectionnelle** ("*one-way function*"), munie d'une **porte arrière** ("*one-way trapdoor function*").

*Une fonction **unidirectionnelle** est une fonction y = f(x) telle que, si l'on connaît la valeur y, il est pratiquement impossible de calculer la valeur x (c'est-à-dire d'inverser la fonction f).*

*On dit que cette fonction est **munie d'une porte arrière** s'il existe une fonction x = g(y, z) telle que, si l'on connaît z, il est facile de calculer x à partir de y. Z est appelée trappe.*

Exemple de scénario d'échange

Bob veux recevoir des messages codés **d'Alice**, il souhaite que ces messages soient indéchiffrables pour **Oscar** qui a accès à leurs échanges :

- Bob et Alice connaissent la fonction unidirectionnelle f ;
- Bob fournit à Alice sa "clé publique" c.
- f et c peuvent être connus de tout le monde : ils sont connus d'Oscar.

Alice chiffre le message M en utilisant l'algorithme f et la clé c ; ceci fournit un texte T chiffré ayant les apparences d'une suite de caractères choisis au hasard :

T = f(M, c).

*Comme f est une fonction unidirectionnelle, **Oscar** est **incapable** de reconstituer le message même si il connaît l'algorithme f, la clé publique c et le texte T.*

Bob, lui, possède la « clé privée » z qui est **absolument secrète**.

z ouvre la porte arrière de la fonction f et permet de déchiffrer le message en appliquant la fonction g au triplet (T, c, z) : M = g(T, c, z).

Bob peut lire le contenu du message envoyé par Alice !

Chiffrement asymétrique : une métaphore avec des cadenas et des valises

Des clé et des cadenas

Alice :
- crée une **clé aléatoire** (la clé privée) ;
- puis fabrique un grand **nombre** de **cadenas** (clé publique) qu'elle met à disposition dans un casier accessible par tous (le casier joue le rôle de canal non sécurisé).

Bob :
- prend un **cadenas** (ouvert) ;
- ferme une **valisette** contenant le document qu'il souhaite envoyer ;
- envoie la valisette à Alice, propriétaire de la clé publique (le cadenas).
  Cette dernière pourra ouvrir la valisette avec sa clé privée

Chiffrement asymétrique

Les contraintes pour un tel algorithme

Il faut trouver un **couple** de fonctions **f** (fonction unidirectionnelle) et **g** (fonction de porte arrière) :

C'est un problème mathématique difficile !

Au départ, le système à clé publique n'a d'abord été qu'une idée dont la faisabilité restait à démontrer.

Des algorithmes ont été proposés par des mathématiciens

Un des premiers algorithmes proposé repose sur la **factorisation** du **produit** de **deux** grands **nombres entiers**.
Cette factorisation demanderait un temps de calcul de plusieurs millions d'années.

Le problème est résolu !

Cet algorithme a été proposé par Rivest, Shamir et Adleman en 1977, ce qui a donné naissance à RSA.

L'idée générale est la suivante :

- la **clé publique** c est le produit de deux **grands nombres entiers**;
- la clé **privée** z est l'un de ces deux nombres entiers;
- g comporte la factorisation de c.

Seul Bob, qui connaît z, peut factoriser c et donc déchiffrer le message chiffré.

Chiffrement asymétrique

Un dernier problème pour la route…

Le système de chiffrement à clé publique est **universel** si chacun publie sa clé publique dans un **annuaire**.

Pour envoyer un message chiffré à Bob, il suffit de trouver sa clé publique dans l'annuaire et de s'en servir pour chiffrer le message avant de le lui envoyer (seul Bob pourra déchiffrer le message).

Il faut bien sûr que **l'annuaire** soit **sûr**.

Oscar peut avoir substitué sa propre clé publique à celle de Bob afin de pouvoir lire les messages destinés à Bob.

Il peut même les renvoyer à Bob une fois lu !

Quelques éléments de réflexion

Tout ce qui a été fait doit être défait.
Nécessité funeste.
Il y a entre l'avenir et nous une interposition fatale. Victor Hugo.

La notion d'inverse

Ce que fait l'algorithme de chiffrement devra être défait plus tard lors du déchiffrement.
En mathématique, l'idée de défaire est **l'inverse**.

Il existe des **fonctions inverses** et des **nombres inverses**.
Les fonctions inverses sont des paires d 'opérations : exemple la multiplication et la division sont des fonctions inverses, ce que l'une fait, l'autre le défait.

Exemple : 5 * 2 = 10, 10 / 2 = 5

Les nombres inverses sont des paires de nombres, ce qu'un nombre fait, l'autre le défait.

Exemple : 2 et ½ avec 5 * 2 = 10, et 10 * ½ = 5

Avec les nombres inverses, l'opération reste la même (ici, la multiplication).

La notion de nombre premier

Un nombre premier est simplement un nombre qui ne possède que deux facteurs, 1 et lui-même.
7 est premier car aucun nombre autre que 1 et 7 ne donne un résultat entier en divisant 7.

Deux nombres sont premiers entre eux s'ils n'ont pas d'autre facteur que 1.
*38 et 55 sont premiers entre eux, alors qu'aucun n'est premier : 38 = 2 * 19 *1 et 55 = 5 * 11 * 1*
*22 et 55 ne sont pas premiers entre eux, car 22 = 2 * 11 et 55 = 5 * 11*

Quelques éléments et rappels de math

Le calcul de l'exponentielle

$X^Y * X^Z = X^{Y+Z}$

$(X^Y)^Z = X^{Y*Z}$

La méthode **indienne** :

soit le calcul de $V = A^B$:

> Initialiser V = 1
> Tant que B ≥ 1
> - si B est impair, multiplier V par A et retrancher 1 à B
> - sinon, élever A au carré et diviser B par 2

Exemple : $V = 6^{35}$

étape 0 : V = 1, B = 35, A = 6
étape 1 : B est impair alors V = 1 * 6 = 6, B = 34
étape 2 : B est pair A = 6 * 6 = 36, B = 17, V = 6
étape 3 : B est impair V = 6 * 36 = 216, B = 16, A = 36
étape 4 : B est pair A = 36 * 36 =1296, B = 8, V = 216
étape 5 : B est pair A = 216 * 216 =1679616, B = 4, V = 216
étape 6 B est pair A = 1679616^2 = 2821109907456, B= 2, V = 216
étape 7 : B est pair A = 2821109907456^2 = 7958661109946400884391936, B= 1
étape 8 : B est impair, V = 216 * A = 1719070799748422591028658176

Calcul de l'exponentielle

Si on décompose l'exposant en binaire

Initialiser V = 1
Pour chaque bit de l'exposant B, en commençant par les poids forts :
- élever V au carré
- si ce bit vaut 1, multiplier V par A

Exemple : 35 = 100011
soit :

étape 0 : V = 1, A = 6
étape 1 : V = (1*1) * 6 = 6 (bit à 1)
étape 2 : V = 6 * 6 = 36 (bit à 0)
étape 3 : V = 36 * 36 = 1296 (bit à 0)
étape 4 : V = 1296 * 1296 = 1679616 (bit à zéro)
étape 5 : V = 1679616 * 1679616 * 6
= 2821109907456 * 6 = 16926659444736 (bit à 1)
étape 6 :V = 16926659444736^2 * 6 = 1719070799748422591028658176

Quelques rappels suite

Division et reste : le modulo

une pendule est modulo 24 : 23h +2h = 1h du matin (arrivé à 24h, le *module*, on recommence !)

La division de l'école :

Valeur / diviseur = quotient & reste

13 / 10 = 1 & 3

34 / 10 = 3 & 4

Arithmétique modulaire

13 mod 10 = 3

34 mod 10 = 4

A mod B est le reste de la division entière de A par B

Exemples :

13 mod 10 = 3	13 mod **10** = 3	13 mod 10 = 3
13 mod 11 = 2	21 mod **10** = 1	14 mod 10 = 4
13 mod 12 = 1	25 mod **10** = 5	14 mod 11 = 3
13 mod 13 = 0	32 mod **10** = 2	15 mod 11 = 4
13 mod 14 = 13	4567 mod **10** = 7	15 mod 12 = 3
13 mod 15 = 13	1247 mod **10** = 7	28 mod 12 = 4

En mathématique modulaire, on ne travaille que sur des entiers **positifs**, **inférieurs** au **module**

La multiplication et le modulo

(A mod B) (C mod B) = A * C mod B

L'exponentielle et le modulo

a^n mod m = (a mod m)^n mod m

Exponentiation modulaire

Calcul de 10 ^ 999 mod 257

Décomposition de l'exposant :

999 = 499 * 2 + 1
499 = 249 * 2 + 1
249 = 124 * 2 + 1
124 = 62 * 2
62 = 31 * 2
31 = 15 * 2 + 1
15 = 7 * 2 + 1

1. $10^{7} \equiv 130 \pmod{257}$
2. $10^{15} \equiv 130 \times 130 \times 10 \equiv 151 \pmod{257}$
3. $10^{31} \equiv 151 \times 151 \times 10 \equiv 51 \pmod{257}$
4. $10^{62} \equiv 51 \times 51 \equiv 31 \pmod{257}$
5. $10^{124} \equiv 31 \times 3 \equiv 190 \pmod{257}$
6. $10^{249} \equiv 190 \times 190 \times 10 \equiv 172 \pmod{257}$
7. $10^{499} \equiv 172 \times 172 \times 10 \equiv 33 \pmod{257}$
8. $10^{999} \equiv 33 \times 33 \times 10 \equiv 96 \pmod{257}$

Et en binaire ?

L'exposant en binaire

999 = 1111100111

10 ^999 mod 257

Reprendre la méthode d'exponentiation binaire est incorporer le modulo !

> Initialiser V = 1
> Pour chaque bit de l'exposant B, en commençant par les poids forts :
> - élever V au carré mod n
> - si ce bit vaut 1, multiplier V par A mod n

Exemple :

étape 0 : V = 1, A = 10
étape 1 :
étape 2 :
étape 3 :
étape 4 :
étape 5 :
étape 6 :
étape 7 :
étape 8 :
étape 9 :
étape 10 :

Et en binaire ?

L'exposant en binaire

999 = 1111100111

10 ^999 mod 257

Reprendre la méthode d'exponentiation binaire est incorporer le modulo !

> Initialiser V = 1
> Pour chaque bit de l'exposant B, en commençant par les poids forts :
> - élever V au carré mod n
> - si ce bit vaut 1, multiplier V par A mod n

Exemple :

étape 0 : V = 1, A = 10
étape 1 : V = (1*1) * 10 = 10 mod 257 (bit à 1)
étape 2 : V = 10 * 10 * 10 = 229 mod 257 (bit à 1)
étape 3 : V = 229 * 229 * 10 = 130 mod 257 (bit à 1)
étape 4 : V = 130 * 130 * 10 = 151 mod 257 (bit à 1)
étape 5 : V = 151 * 151 * 10 = 51 mod 257 (bit à 1)
étape 6 : V = 51 * 51 = 31 mod 257 (bit à 0)
étape 7 : V = 31 * 31 = 190 mod 257 (bit à 0)
étape 8 : V = 190 * 190 * 10 = 172 mod 257 (bit à 1)
étape 9 : V = 172 * 172 * 10 = 33 mod 257 (bit à 1)
étape 10 :V = 33 * 33 * 10 = 96 mod 257 (bit à 1)

Quelques remarques sur les mathématiques modulaires

Utilisation de nombre premier

Lorsque le module est premier, les opérations « se comportent » de **manière pratique**.

Pierre **Fermat** au XVI^{e} siècle :

Si on utilise un nombre premier comme module, alors quand on élève un nombre à la puissance (nombre premier -1), on obtient 1 !

Pour n'importe quel nombre m et pour p premier :

$$\mathbf{m^{(p-1)} \bmod p = 1}$$

Exemple : $7^{10} \bmod 11 = 1$ …pas besoin de calcul car 11 est premier !

Leonhard **Euler** :

Lorsqu'on utilise un module comme étant le produit de deux nombres premiers on a :

Soit $n = p * q$, avec p et q premiers, et quelque soit m

$$\mathbf{m^{(p-1)(q-1)} \bmod n = 1}$$

Exemple : soit p = 11 et q = 5, n = 55 et (p – 1)(q – 1) = 10 * 4 = 40

$38^{40} \bmod 55 = 1$...pas besoin de calcul !

Si on manipule le résultat d'Euler en multipliant par m l'équation :

$$m * m^{(p-1)(q-1)} \bmod n = m$$

$$m^{(p-1)(q-1)+1} \bmod n = m$$

Cela veut dire que si on éléve m à une certaine puissance, on retombe sur m !

Ainsi, il est possible de « **cycler** » dans les exponentiations :

Exemple :

7^1 = 7 mod 55,
7^2 = 49 mod 55,
7^3 = 7*49 = 343 = 13 mod 55,
7^4 = 13 * 7 = 91 = 36 mod 55, …

7^40 = 1 mod 55
7^41 = 7 mod 55
7^42 = 49 mod 55
7^43 = 13 mod 55...

Idée de chiffrement à clé publique : le RSA

Euler modifié

On sait que $m^{(p-1)(q-1)+1} \bmod n = m$

Il est possible d'aller de m vers m par (p – 1)(q – 1) + 1, il ne suffit plus que de décomposer cette valeur en deux sous valeurs :

- l'une permettant de passer de m à une valeur intermédiaire ;
- l'autre permettant de passer de cette valeur intermédaire vers m ;

Possibilité de chiffrement à clé publique !

e * d = (p – 1)(q – 1) + 1

Exemple : e * d = 41...mais 41 est premier !

Comment faire ?

utiliser l'arithmétique modulaire : trouver e * d tel que e * d = 1 mod { e * d – 1}

Principe de RSA

utiliser deux modules, l'un pour les clès et l'autre pour chiffrer.

pour les clés : (p – 1) (q – 1)

pour chiffrer p * q

Chiffrement asymétrique : présentation de RSA

Un algorithme simple

Soient :

- **M** le message en clair
- **C** le message encrypté
- **(e,n)** constitue la clé publique
- **(d,n)** constitue la clé privée
- **n** le produit de 2 nombres premiers
- **^** l'opération de mise à la puissance (a^b : a puissance b)
- **mod** l'opération de modulo (*reste de la division entière*)

Pour chiffrer un message M, on fait: C = M^e mod n

Pour déchiffrer: M = C^d mod n

Construction des clés

Pour créer une paire de clés, c'est très simple, mais il ne faut pas choisir n'importe comment e,d et n.

Le calcul de ces trois nombres est délicat.

- prendre deux nombres premiers p et q (de taille à peu près égale). Calculer n = pq.
- prendre un nombre e qui n'a aucun facteur en commun avec (p-1)(q-1).
- calculer d tel que e * d mod (p-1)(q-1) = 1

Le couple (e,n) constitue la clé publique. (d,n) est la clé privée.

La puissance du cryptage RSA est en effet basée sur la difficulté de factoriser un grand entier. C'est pour cela que l'on choisit des nombres premiers p et q d'environ 100 chiffres, pour rendre la factorisation hors de portée, même des meilleurs ordinateurs.

Exemple d'utilisation de RSA

Création de la paire de clés:

Soient deux nombres premiers au hasard: p = 29, q = 37, on calcule n = pq = 29 * 37 = 1073.

On doit choisir e au hasard tel que e n'ai aucun facteur en commun avec (p-1)(q-1):
(p-1)(q-1) = (29-1)(37-1) = 1008
On prend e = 71
On choisit d tel que 71*d mod 1008 = 1, on trouve d = 1079.

On a maintenant les clés :

- la **clé publique** est (e,n) = (71,1073) (=*clé de chiffrement*)
- la **clé privée** est (d,n) = (1079,1073) (=*clé de déchiffrement*)

Chiffrement du message 'HELLO'.

On prend le code ASCII de chaque caractère et on les met bout à bout:
m = 7269767679
Il faut découper le message en blocs qui comportent moins de chiffres que n.
n comporte 4 chiffres, on découpe notre message en blocs de 3 chiffres:

726 976 767 900 (on complète avec des zéros)

On chiffre chacun de ces blocs :
726^71 mod 1073 = 436
976^71 mod 1073 = 822
767^71 mod 1073 = 825
900^71 mod 1073 = 552
Le message chiffré est 436 822 825 552.

Exemple d'utilisation de RSA

On peut le déchiffrer avec d:

436^1079 mod 1073 = 726
822^1079 mod 1073 = 976
825^1079 mod 1073 = 767
552^1079 mod 1073 = 900

C'est à dire la suite de chiffre 726976767900.
On retrouve notre message en clair 72 69 76 76 79 : 'HELLO' !

Propriété unique

L'algorithme a la propriété spéciale suivante (*utilisé* pour l'authentification):

chiffrement (déchiffrement (M)) = déchiffrement (chiffrement (M))

C'est-à-dire que l'utilisation de sa clé privée pour chiffrer un message M permet de construire un message M' qui peut être déchiffré par sa clé publique...ainsi il est possible de prouver que l'on dispose bien de la clé privée qui correspond à la clé publique !

Sécurité

La force du chiffrement dépend de la longueur de la clé utilisée.

Ce protocole a l'avantage d'utiliser des clés de longueur variable de 40 à 2 048 bits ;
Il faut actuellement utiliser une clé au minimum de 512 bits (Six laboratoires ont dû unir leurs moyens pour casser en août 1999 une clé à 512 bits)

Le cryptage à clé symétrique - le DES

Un standard de chiffrement

Développé dans les années 70 par IBM, la méthode DES fut adoptée et rendue standard par le gouvernement des Etats Unis.

Il devait répondre à l'époque aux critères suivants :

- avoir un haut niveau de sécurité lié à une clé de petite taille servant au chiffrement et au déchiffrement,
- être compréhensible,
- ne pas dépendre de la confidentialité de l'algorithme,
- être adaptable et économique,
- être efficace et exportable.

La méthode DES utilise des clés d'une taille de 56 bits ce qui la rend de nos jours facile à casser avec les nouvelles technologies de cryptanalyse. Mais elle est toujours utilisée pour des petites tâches tel que l'échange de clés de cryptage (technologie SSL).

La clé est sur 64bits dont 8 sont utilisés comme calcul de l'intégrité des 56 autres (parité).

Le DES est un standard utilisé depuis plus de 20 ans.

Il a suscité de nombreuses critiques, des suspicions de vulnérabilité à l'attaque de son algorithme, mais n'a pas eu d'alternatives jusqu'à ces dernières années : modifié par la NSA, trafiqué par IBM, …

Le DES ou un algorithme de chiffrement par confusion

Principe de l'algorithme

C'est un algorithme à base de :

- **décalage** ;
- « **ou exclusif** » ;
- **transposition/recopie** (appelé *expansion*).

Ces opérations sont **faciles** à réaliser par un processeur.

Le chiffrement par DES est très rapide.

Certaines puces spécialisées chiffrent jusqu'à 1 Go de données par seconde ce qui est énorme : *c'est plus que ce qu'est capable de lire un disque dur normal*.

DES : l'algorithme

Principe de fonctionnement

L'algorithme utilise une clé de 56 bits.

Décomposition du texte en clair en bloc

- le texte en clair est découpé en bloc de 64 bits qui seront chiffrés un par un ;

Utilisation en différentes étapes, éventuellement répétées (en tout *19 étapes) :*

- la première étape **transpose** chaques blocs de 64 bits du texte en clair avec la clé de 56 bits ;
- 16 **étapes intermédiaires** ;
- l'avant dernière étape **intervertit** les 32 bits de droite et de gauche ;
- la dernière étape **transpose** chaques blocs de 64 bits du texte avec la clé de 56 bits (*exactement à l'inverse de la première étape*).

Les 16 étapes intermédiaires sont identiques mais varient par différentes utilisations de la clé

Une étape intermédiaire

Elle consiste à couper le bloc de 64 bits en 2 blocs de 32 bits.

Le bloc de sortie de gauche sera une recopie du bloc de droite en entrée.

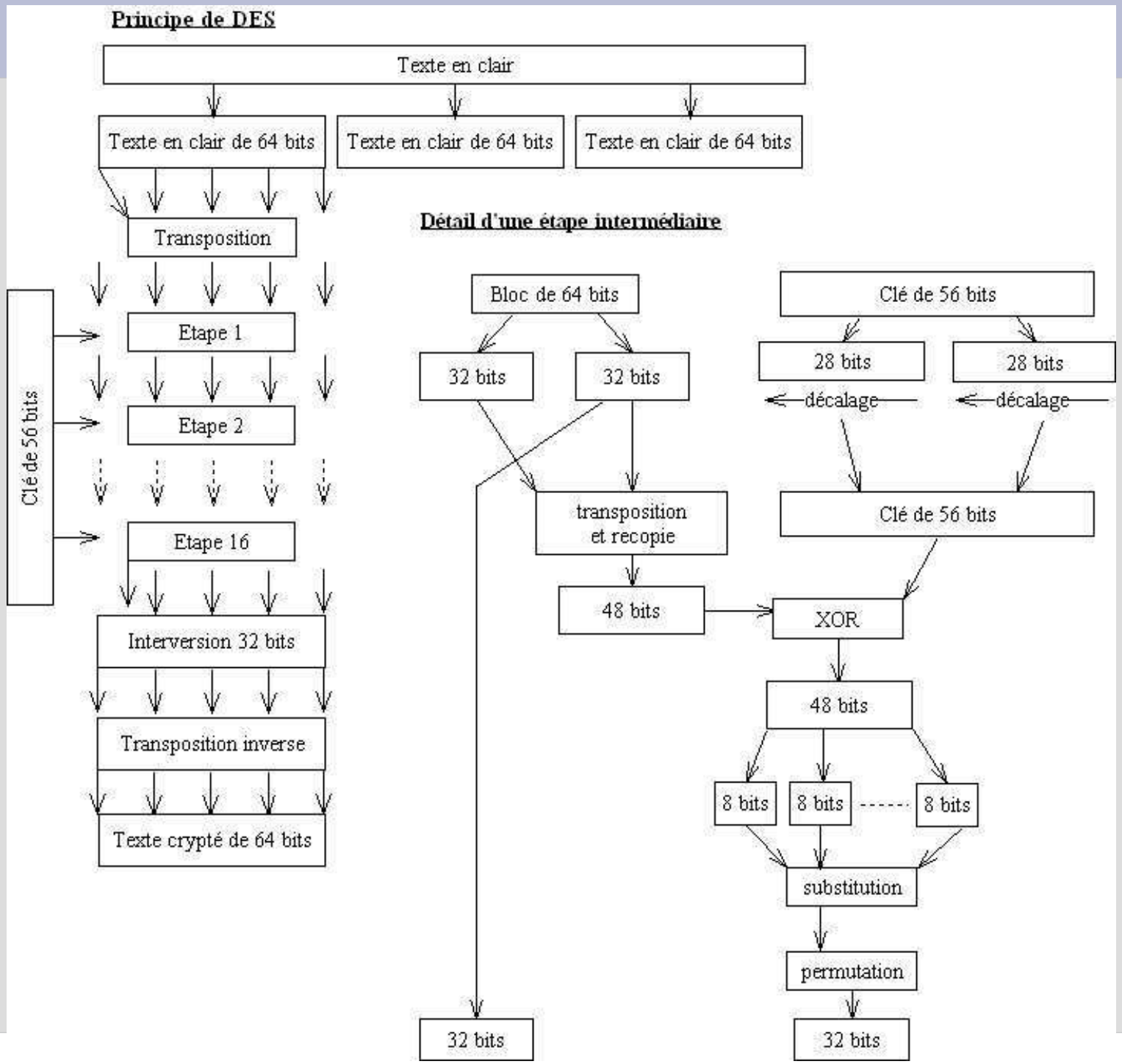
Le bloc de droite est utilisé pour calculer un nombre de 48 bits à l'aide de **règles** de **transposition** et de **recopie**.

*Ces règle sont **stockées** dans des **tables** et leur construction reste mystérieuse…le NSA y a participé !*

La clé de 56 bits est divisée en 2 blocs de 28 bits, sur ces blocs de 28 bits un **décalage circulaire** est effectué vers la gauche d'un **nombre de position** dépendant de l'itération.

Un « ou exclusif » est calculé entre le nombre de 48 bits et la clé de 56 bits.

Le résultat de ces « ou exclusifs » est découpé en blocs de 6 bits.


Principe de DES
Texte en clair
Texte en clair de 64 bits
Texte en clair de 64 bits
Texte en clair de 64 bits
Transposition
Clé de 56 bits
Etape 1
Etape 2
Etape 16
Interversion 32 bits
Transposition inverse
Texte crypté de 64 bits
Détail d'une étape intermédiaire
Bloc de 64 bits
32 bits
32 bits
transposition
et recopie
48 bits
Clé de 56 bits
28 bits
28 bits
décalage
décalage
Clé de 56 bits
XOR
48 bits
8 bits
8 bits
8 bits
substitution
permutation
32 bits
32 bits

Le cryptage à clé symétrique - le DES

La cryptanalyse ?

Brute force : essayer toutes les clés possibles !

Le **nombre** de **clés** est **élevé** (2^56=7,2*10 ^{16}) et peut être facilement augmenté en changeant le nombre de bits pris en compte (soit exactement 72.057.595.037.927.936 clés différentes !).

Exemple : si une personne peut tester 1 million de clés par seconde

il lui faut **1000 ans** pour tout essayer !

La loi de Moore : énoncée par Gordon Moore en 70 :

« le nombre de transistors d'une puce doublerait tous les 18 mois à coût constant »

1975 : un ordinateur a besoin de 100 000 jours (300 ans) pour tester toutes les clés...

2000 : un ordinateur 100 000 fois plus puissant a besoin de 1 jour (un ordinateur à 200 K€) !

Challenge DES : proposé par la société RSA en janvier 1997

- cassage du DES en 96 jours ;
- février 98, cassage en 41 jours ;
- juillet 98, cassage en 56 heures sur une machine de moins de 60k€ ;
- janvier 99, cassage en moins de 24h !

Le DES a été cassé grâce aux méthodes de **cryptanalyse différentielle** et à la puissance coordonnées des machines mises à disposition par un état par exemple.

Les évolutions

Si un algorithme est « *usé* » il est possible d'utiliser des **clés plus longues**.

Le TDES (*Triple DES*) a été créé pour pallier les limites du DES, par l'utilisation d'une chaîne de trois chiffrements DES à l'aide de seulement deux clés différentes :

Chiffrement avec une clé C1-> **déchiffrement** avec une clé C2 -> **chiffement** avec la clé C1

L'avenir ?

Le DES et le TDES sont amenés à être remplacé par un nouvel algorithme : le **Rijndael** (du nom de ses inventeurs) qui a été sélectionné pour devenir AES.

Chiffrement à clé symétrique - Autres algorithmes

IDEA (International Data Encryption Algorithm)

- conçu dans les années 90 par deux chercheurs suisses (Lai et Massey) de l'ETH (Eidgenössische Technische Hochschule) de Zurich, IDEA (International Data Encryption Algorithm) ;
- utilise une clé de **128 bits** ;
- résistera encore pendant quelques dizaines d'années aux attaques cryptanalytiques.

Aucune attaque existe contre l'IDEA.
IDEA est breveté aux Etats-Unis et dans de nombreux pays européens.
IDEA est gratuit tant que son utilisation reste non commerciale.

Blowfish

- développé par Bruce Schneier ;
- blowfish travaille par bloc de 64 bits en utilisant une clé variable pouvant aller jusqu'à **448 bits** ;
- il n'existe aucun moyen de casser cet algorithme.

Blowfish est utilisé dans différents logiciels tel que NAUTILUS ou PGPFONE

RC4 (Rivest Cipher 4)

- algorithme de cryptage très rapide ;
- utilisé dans de multiples applications telles que les communications sécurisées pour crypter le trafic transitant entre des interlocuteurs ;
- RC4 est basé sur l'utilisation de **permutations aléatoires**.

Le gouvernement des Etats-Unis autorise l'exportation du RC4 avec des clés de 40 bits.
Problème : un **flux chiffré** avec 2 clés identiques sera facilement cassable.

Chiffrement à clé symétrique - Autres algorithmes

AES (Advanced Encryption Standard)

L'AES est un standard de cryptage symétrique destiné à remplacer le DES (Data Encryption Standard) qui est devenu trop faible au regard des attaques actuelles.

L'AES
- est un standard, libre d'utilisation, sans restriction d'usage ni brevet ;
- est un algorithme de chiffrement par blocs (comme le DES) ;
- supporte différentes combinaisons [longueur de clé]-[longueur de bloc] :
  128-128, 192-128 et 256-128 bits

Le choix de cet algorithme répond à de nombreux critères tels que :
- la **sécurité** ou l'effort requis pour une éventuelle cryptanalyse ;
- la **facilité** de **calcul** : cela entraîne une grande rapidité de traitement ;
- les **faibles besoins** en ressources : mémoire très faibles ;
- la **flexibilité d'implémentation** : cela inclut une grande variété de plates-formes et d'applications ainsi que des tailles de clés et de blocs supplémentaires (il est possible d'implémenter l'AES aussi bien sous forme logicielle que matérielle, câblé) ;
- la simplicité : le design de l'AES est relativement simple.

Chiffrement à clé publique *versus* chiffrement à clé secrète

Remarques sur le chiffrement à clé publique

L'utilisation de tels codes de chiffrement est coûteuse, ils ne peuvent pas être appliqué sur un grand débit de données à transmettre.

Principaux algorithmes utilisés : **RSA**, Rivest, Shamir et Adelman 1978.
El Gamal 1981.

Remarques sur le chiffrement à clé privée

Difficulté du partage des clés, ainsi que la multiplication des clés quand plusieurs interlocuteurs sont en contact.

Dans un réseau de 5 personnes communicant entre elles il faut n(n-1)/2 clés, soient 10 clés différentes..

Comparaisons entre RSA et DES

RSA

- clé de 40 bits
- chiffrement matériel : 300 Kbits/sec
- chiffrement logiciel : 21,6 Kbits/sec
- **Inconvénient majeur** : un pirate substitue sa propre clé publique à celle du destinataire, il peut alors intercepter et décrypter le message pour le recoder ensuite avec la vraie clé publique et le renvoyer sur le réseau. **« L'attaque » ne sera pas décelée.**
- **usage** : on ne les emploiera que pour transmettre des données courtes (de quelques octets) telles que les clés privées et les signatures électroniques.

DES

- clé de 56 bits
- chiffrement matériel : 300 Mbits/sec
- chiffrement logiciel : 2,1 Mbits/sec
- **Inconvénient majeur** : attaque « brute force » rendue possible par la puissance des machines.
- **Usage** : chiffrement rapide, adapté aux échanges de données de tous les protocoles de communication sécurisés.

Comparaison et combinaison

La sécurité offerte par le chiffrement à clé

La sécurité d'un code à clé est **proportionnelle** à la taille de la clé employée, c-à-d. plus la clé est longue plus il faut de calcul et donc de temps pour arriver à le casser.

Chiffrement par substitution : 26 lettres possibles associables, soit 26! (factorielle 26) soient 291 461 126 605 635 584 000 000 possibilités ! mais **l'analyse fréquentielle**...

Le chiffrement à clé : il **protège** des analyses fréquentielles ;

Attaque « brute force » : essayer toutes les clé possibles pour déchiffrer le message chiffré, donc plus la clé est longue (nombre de bits) plus il y a de clé à essayer (2 fois plus de clé à essayer pour chaque bit ajouté !).

La force de la sécurité est à mettre en rapport avec le type de données à sécuriser :
– une **transaction bancaire** doit être sécurisée pendant **quelques minutes**
– un **document secret d'état** doit pouvoir être protégé plus de 50 ans par exemple.

La vitesse

Il existe un **décalage** de **puissance** de calcul pour le chiffrement/déchiffrement des codes à clé secrète (algorithme de cryptage symétrique de type DES) et à clé publique (algorithme de cryptage asymétrique de type RSA).

Code à clé secrète : applicable à un débit de données supérieur.

C'est pourquoi seule l'utilisation de code à clé secrète est «réaliste» pour sécuriser une transaction entre deux utilisateurs sur Internet.

Résolution du problème de l'échange des clés secrètes :

utilisation d'une méthode **hybride** combinant à la fois chiffrement **symétrique** et **asymétrique**.

Le chiffrement par bloc

Le chiffrement par bloc est la manière choisie pour chiffrer le message décomposé en bloc, c-à-d. dans **quel ordre** et après quel transformation chaque bloc va être chiffré. On parlera de mode d'opérations.

Quatres modes définis

Quatre modes sont définis dans FIPS 81, Federal Information Processing Standards Publication 81, (2 décembre 1980) et aussi dans la norme ANSI X3.106-1983.

- Electronic Code Book (**ECB**) ;
- Cipher Block Chaining (**CBC**) ;
- Cipher FeedBack (**CFB**) ;
- Output FeedBack (**OFB**).

ECB : Electronic Codebook

Mode d'opération normal : il applique l'algorithme au texte clair en transformant normalement chaque bloc de texte clair.

T[n] = nième bloc de texte en clair.
C[n] = nième bloc de texte chiffré.
E(m) = fonction de chiffrement du bloc m.
D(m) = fonction de déchiffrement du bloc m.

Chiffrement : C[n] = E(T[n])
Déchiffrement : T[n] = D(C[n])
T et C sont d'une longueur fixe.

Problèmes :

- si on utilise deux fois le même texte clair et la même clé de chiffrement, le résultat du chiffrement sera identique.
- il faut un nombre suffisant d'octets de texte en clair (huit octets pour le DES par exemple) avant de commencer.

Le chiffrement par bloc

CBC : Cipher Block Chaining

C'est un des modes les plus populaires.

Il apporte une solution au premier problème du mode ECB :

- avant d'être chiffré, l'opération binaire « XOR » est appliquée entre le bloc actuel de texte en clair et le bloc précédent de texte chiffré ;
- pour le tout premier bloc, un bloc de contenu aléatoire est généré et utilisé, appelé « **vecteur d'initialisation** » (initialization vector, ou IV).

Ce premier bloc est envoyé tel quel avec le message chiffré.

T[n] = nième bloc de texte en clair.
C[n] = nième bloc de texte chiffré.
VI = vecteur d'initialisation

E(m) = fonction de chiffrement du bloc m.
D(m) = fonction de déchiffrement du bloc m.

Chiffrement : C[0] = E(T[0] xor VI)
C[n] = E(T[n] xor C[n-1]) , si (n > 0)

Déchiffrement : T[0] = D(C[n]) xor VI
T[n] = D[C[n]) xor C[n-1] , si (n > 0)

T et C sont d'une longueur fixe

Le chiffrement par bloc

CFB : Cipher Feedback

Le mode qui semble éviter tous les problèmes est le CFB.
L'opération XOR est appliquée entre le bloc de texte clair et le résultat précédent chiffré à nouveau par la fonction de chiffrement.
il offre une grande sécurité.
Pour le premier bloc de texte clair, on génère un vecteur d'initialisation.

T[n] = nième bloc de texte clair.
C[n] = nième bloc de texte chiffré.
VI = vecteur d'initialisation

I[n] = nième bloc temporaire
E(m) = fonction de chiffrement et de déchiffrement du bloc m

Chiffrement :
I[0] = VI
I[n] = C[n-1] , si (n > 0)
C[n] = T[n] xor E(I[n])

Déchiffrement :
I[0] = VI
I[n] = C[n-1], si (n > 0)
T[n] = C[n] xor E(I[n])

T et C sont d'une longueur fixe

La fonction de chiffrement et de déchiffrement est la même.

Le chiffrement par bloc

OFB : Output Feedback

Le mode OFB est une solution aux deux problèmes relatifs au mode ECB.
Au départ un vecteur d'initialisation est généré.
Ce bloc est chiffré à plusieurs reprises et chacun des résultats est utilisé successivement dans l'application de l'opération XOR avec un bloc de texte en clair.
Le vecteur d'initialisation est envoyé tel quel avec le message chiffré.

T[n] = nième bloc de texte en clair.
C[n] = nième bloc de texte chiffré.
E(m) = fonction de chiffrement et de déchiffrement du bloc m
I[n] = nième bloc temporaire
R[n] = nième bloc temporaire second
VI = vecteur d'initialisation

Chiffrement :
I[0] = VI
I[n] = R[n-1] , si (n > 0)
R[n] = E(I[n])
C[n] = T[n] xor R[n]

Déchiffrement :
I[0] = VI
I[n] = R[n-1] , si (n > 0)
R[n] = E(I[n])
T[n] = C[n] ^ R[n]

T et C sont d'une longueur fixe

Problèmes :

- le texte en clair est seulement soumis à un XOR.
  Si le texte clair est connu, un tout autre texte en clair peut être substitué en inversant les bits du texte chiffré de la même manière qu'inverser les bits du texte clair (bit-flipping attack).
- il existe une petite possibilité qu'une clé et un vecteur d'initialisation soient choisis tels que les blocs successifs générés puissent se répéter sur une courte boucle.

Le mode OFB est souvent utilisé comme générateur de nombre aléatoire.

Le chiffrement par flux

Définition

Les algorithmes de chiffrement par flux peuvent être vu comme des algorithmes de chiffrement par bloc où le bloc a une dimension unitaire (1 bit, 1 octet…) ou relativement petite.
Ils sont appelés *stream ciphers*.

Avantages :

- la **méthode** de **chiffrement** peut être changée à chaque symbole du texte clair ;
- ils sont **extrêmement rapides** ;
- ils ne propagent pas les erreurs (diffusion) dans un environnement où les erreurs sont fréquentes ;
- ils sont utilisables lorsque l'information ne peut être traitée qu'avec de petites quantités de symboles à la fois (par exemple si l'équipement n'a pas de mémoire physique ou une mémoire tampon très limitée).

Fonctionnement :

Ils appliquent de simples transformations selon un *keystream* utilisé.
Le *keystream* est une **séquence** de **bits** utilisée en tant que clé qui est générée aléatoirement par un algorithme (*keystream generator*).

Propriétés :

Avec un *keystream* choisi aléatoirement et utilisé qu'une seule fois, le texte chiffré est très sécurisé.
La génération du keystream peut être :

- **indépendante** du texte en clair et du texte chiffré, appelée chiffrement de flux synchrone (synchronous stream cipher) ;
- **dépendante** (self-synchronizing stream cipher).

Les chiffrements de flux les plus répandus sont synchrones

Algorithmes les plus connus :

LFSR (Linear Feedback Shift Register), rapide mais vulnérable à l'heure actuelle.
RC4, inventé par Ron Rivest en 87 (société RSA), utilisé dans le protocole SSL et Oracle Secure SQL.
SEAL (Software-optimized Encryption Algorithm), Don Coppersmith et Phillip Rogaway en 93 (IBM), plus rapide que RC4.

.

Echange sécurisé

L'utilisation d'algorithme de chiffrement à clé symétrique n'est pas réaliste d'un point de vue de la puissance de calcul nécessaire.
Cette **puissance augmente** en **même temps** qu'il est nécessaire d'améliorer la sécurité de ces algorithmes (augmentation de la taille des clé) : le **décalage reste** !
Il existe alors soit à trouver un moyen de partager secrétement une même clé secrète ou bien à combiner les deux :
l'échange de la clé secrète d'un algorithme de chiffrement symétrique est « protégé » par un algorithme de chiffrement asymétrique.

Avantages :

- la clé secréte est chiffrée et échangée ;
- après l'échange on bascule le chiffrement en utilisant un algorithme symétrique plus rapide ;
- on démarre l'échange avec l'utilisation d'un algorithme asymétrique qui possède l'avantage d'offrir un moyen d'identifier les interlocuteurs.
  L'algorithme RSA a la propriété chiffrement(déchiffrement(M)) = déchiffrement(chiffrement(M)).

Échange sécurisé d'information

Cet échange se déroule en 2 phases :

- échange sécurisé d'une clé secrète pour la session, appelée également «clé de session»
- échange sécurisé des messages à l'aide d'un algorithme à clé secrète.

Une phase d'authentification des interlocuteurs peut être ajoutées au début.

Clé de session

C'est un compromis entre le chiffrement symétrique et asymétrique permettant de combiner les deux techniques.

Il existe deux méthodes :
Première possibilité :

- générer aléatoirement une clé de **taille raisonnable** utilisée pour un algorithme de cryptage symétrique;
- chiffrer cette clé à l'aide d'un algorithme de cryptage à clé publique (à l'aide de la clé publique du destinataire) ;

Cela impose que l'un des interlocuteurs possède la clé publique de l'autre (pas toujours facile de s'assurer que la clé publique appartient bien à la bonne personne).

Seconde possibilité :

- construire une clé de session à l'aide de la méthode d'échange des clés de **Diffie-Hellman**.
- les interlocuteurs n'ont pas besoin de **partager** une **clé publique** avant de commencer leur communication chiffrée !

Cette méthode est extrémement employée pour initier un canal de transmission sécurisée avant tout échange.

Les deux interlocuteurs disposent ensuite :

- d'une **clé commune** qu'ils sont seuls à connaître
- de la possibilité de communiquer en chiffrant leur données à l'aide d'un algorithme de chiffrement symétrique rapide.

Echange sécurisé : la méthode Diffie - Hellman

La méthode d'échange des clés de Diffie-Hellman

Alice et Bob se mettent en accord sur deux grands nombres premiers n et g avec (n-1)/2 premier et quelques conditions sur g.
Ces nombres sont publics.
Alice prend le nombre n et Bob le nombre g.

Alice choisit un nombre de 512 bits secret x, Bob fait de même avec y.
Alice envoie à Bob un message contenant le nombre n, le nombre g et le résultat de (g^x mod n)

Bob envoie à Alice le résultat de (g^y mod n)
Alice et Bob calculent (g^y mod n)^x et (g^x mod n)^y
A et B partagent maintenant la même clé secrète g^xy mod n.
Si Oscar, l'intrus capture g et n, il ne peut pas calculer x et y, car il n'existe pas de méthode humainement utilisable pour calculer x à partir de g^x mod n !

Problème : Oscar peut s'insérer entre Alice et Bob et proposé sa valeur z en lieu et place de x pour Bob et de y pour Alice :

Alice	-->	n, g, g^x mod n	-->	Oscar	–>	n, g, g^z mod n	–> Bob
	<–	g^z mod n	<--		<–	g^y mod n	<–

Conclusion : il faut une phase **préliminaire d'authentification** !

L'authentification

L'authentification est suivie par l'autorisation

L'autorisation définit les ressources, services et informations que la personne identifiée peut utiliser, consulter ou mettre à jour, exemple : son courrier électronique, des fichiers sur un serveur FTP…

L'approche traditionnelle

Combinaison d'une identification et d'un mot de passe (code secret personnel).
Le mot de passe doit posséder certaines caractéristiques : non trivial, difficile à deviner, régulièrement modifié, secret…
Des outils logiciel ou hardware de génération de mots de passe existent, mais les mots de passe générés sont difficiles à retenir !

L'approche évoluée, la notion de challenge/réponse

Alice envoie à Bob un **message aléatoire** (challenge)
Chiffement à **clé secrète** :

- Alice et Bob partage une même clé secrète ;
- Bob renvoie à Alice le message **chiffré** à l'aide de la clé secrète (réponse) ;
- Alice peut **déchiffrer** le message chiffré avec la clé secrète...C'est Bob !

Chiffrement à **clé publique** :

- Bob renvoie à Alice le message chiffré à l'aide de sa clé privée (réponse) ;
- exploitation de la propriété chiffrement(déchiffrement(M)) = déchiffrement(chiffrement(M)) ;
- Alice peut déchiffrer ce message chiffré à l'aide de la clé publique de Bob… c'est donc Bob !

Problème : cette méthode permet de faire des attaques sur la clé privée de Bob en soumettant des messages aléatoires bien choisi.
Solution : calculer un «résumé» du message aléatoire initial, un “digest”, et l'utiliser à la place du message aléatoire lors du chiffrement.
L'obtention de ce «résumé» se fait à l'aide d'une fonction de hachage.

Fonction de hachage

Une fonction de hachage est une fonction permettant d'obtenir un résumé d'un texte, c-à-d. une suite de caractères assez courte représentant le texte qu'il résume.
La fonction de hachage doit :

- être telle qu'elle **associe un et un seul** résumé à un texte en clair (cela signifie que la moindre modification du document entraine la modification de son résumé), c-à-d. « **sans collision** ».
- être une **fonction** à **sens unique** (*one-way function*) afin qu'il soit impossible de retrouver le message original à partir du résumé.

y = F(x), mais il est impossible de retrouver x à partir de y !

Propriétés

une fonction de hachage "H" transforme une entrée de données d'une dimension variable "m" et donne comme résultat une sortie de données inférieure et fixe "h" (h = H(m)).

- l'entrée peut être de dimension variable ;
- la sortie doit être de dimension fixe ;
- H(m) doit être relativement facile à calculer ;
- H(m) doit être une fonction à sens unique ;
- H(m) doit être « sans collision ».

Utilisation - Authentification et intégrité

Les algorithmes de hachage sont utilisés :

- dans la génération des signatures numériques, dans ce cas, le résultat "h" est appelé "empreinte" ;
- pour la vérification si un document a été modifié (le changement d'une partie du document change son empreinte) ;
- pour la construction du **MAC**, *Message Authentication Code*, ou code d'authentification de message, il permet de joindre l'empreinte du message chiffré avec une **clé secrète** ce qui protège contre toute modification du message (si l'intrus modifie le message et son empreinte, il est incapable de chiffrée celle-ci pour la remplacer dans le message).

Fonction de hachage

Principaux algorithmes

Il existe différents algorithmes réalisant de traitement :

- **MD2**, **MD4** et **MD5** (MD signifiant Message Digest), développé par Ron Rivest (société RSA Security), créant une empreinte digitale de 128 bits pour MD5.
  Il est courant de voir des documents en téléchargement sur Internet accompagnés d'un fichier MD5, il s'agit du résumé du document permettant de vérifier l'intégrité de ce dernier

- **SHA** (pour Secure Hash Algorithm, pouvant être traduit par Algorithme de hachage sécurisé), développé par le NIST en 1995.
  il crée des empreintes d'une longueur de 160 bits.
  C'est un standard SHA0 et SHA1 (devenu le standard SHS)

- **RACE** Integrity Primitives Evaluation Message Digest, développé par Hans Dobbertin, Antoon Bosselaers et Bart Preneel ;

- **RIPEMD**-128 et RIPEMD-160, créé entre 88 et 92 ;

- **Tiger**, développé par Ross Anderson et Eli Biham, plus rapide que MD5 (132Mb/s contre 37Mb/s sur une même machine, optimisé pour processeur 64bit).

La signature électronique

Le scellement ou sceau ou signature électronique

Il est possible de :

- **joindre** à un **document** sa **signature** obtenue à l'aide d'une fonction de hachage en la chiffrant à l'aide de sa clé privée.

Le document peut être **identifié** comme provenant de la personne (*Authentification*) et cela assure également la **non-répudiation** (utilisation de la clé privée).
Il est possible de déchiffrer cette signature à l'aide de la clé publique de la personne.
Cette signature permet de **contrôler l'intégrité** du document.
La **confidentialité** est assurer par un chiffrement du document.
Il est optionnel car cela nécessite du temps (utilisation d'un chiffrement à clé publique)

Fonctionnement

1. L'expéditeur calcule **l'empreinte** de son **texte en clair** à l'aide d'une fonction de hachage ;
2. L'expéditeur chiffre **l'empreinte** avec sa **clé privée** ;

Le chiffrement du document est optionnel si la confidentialité n'est pas nécessaire.

3. L'expéditeur chiffre le **texte en clair** et **l'empreinte chiffrée** à l'aide de la clé publique du destinataire.
4. L'expéditeur envoie le **document** chiffré au destinataire ;
5. Le destinataire déchiffre le **document** avec sa clé privée ;
6. Le destinataire déchiffre **l'empreinte** avec la **clé publique** de l'expéditeur (authentification) ;
7. Le destinataire calcule **l'empreinte** du **texte clair** à l'aide de la même fonction de hachage que l'expéditeur ;
8. Le destinataire compare les deux empreintes.

Deux empreintes identiques impliquent que le texte en clair n'a pas été modifié (intégrité).

Le standard américain est le **DSS** (Digital Signature Standard), qui spécifie trois algorithmes : le **DSA** (Digital Signature Algorithm), **RSA** et **ECDSA** (Elliptic Curves Digital Signature Algorithm).

Type de signature

Type de signature	Validité	Présomption de fiabilité
Signature électronique	Identification du signataire et intégrité du document	non
Signature électronique sécurisée	Idem + Signature personnelle sous contrôle exclusif	non
Signature électronique sécurisée présumée fiable	Signature sécurisée, utilisant des moyens certifiés et des certificats qualifiés	oui

Authentification et échange sécurisé

Authentification à l'aide du chiffrement à clé publique et échange de clé de session

On suppose que chaque interlocuteur possède la clé publique de l'autre.
Ce qui n'est pas évident…
On désire échanger une clé de session tout en s'assurant de l'identité de chacun.

Scénario : Alice veut échanger avec Bob

- Alice chiffre avec la clé publique de Bob son identité et un nombre aléatoire N ;
- Alice envoie ce message à Bob ;
  Bob qui reçoit ce message ne sait pas s'il vient d'Alice ou bien d'Oscar (l'intrus)
- Bob répond par un message chiffré avec la clé publique d'Alice, contenant : N, un nombre aléatoire P et S une clé de session ;
- Alice reçoit le message et le déchiffre à l'aide de sa clé privée
  Si Alice trouve N alors c'est bien Bob qui lui a envoyé le message puisqu'il était le seul à pouvoir déchiffrer N, *pas d'intrus qui s'insére dans la communication*
  Ce n'est pas possible non plus que cette réponse soit un message déja échangé puisque N vient juste d'être choisi par Alice.
- Alice valide la session en renvoyant à Bob le nombre P chiffré maintenant avec la clé de session S

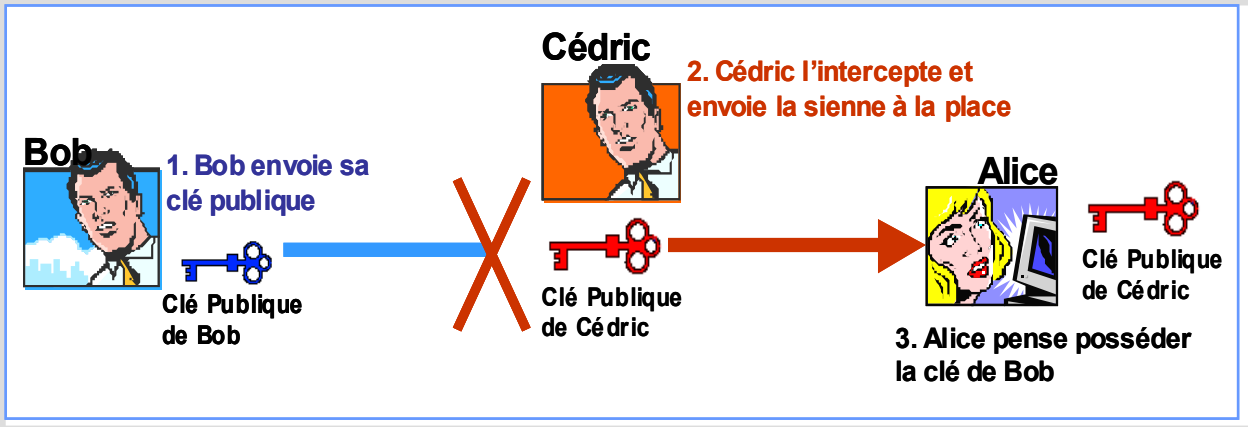
L'échange est maintenant basculé en chiffrement à clé secrète avec la clé S…

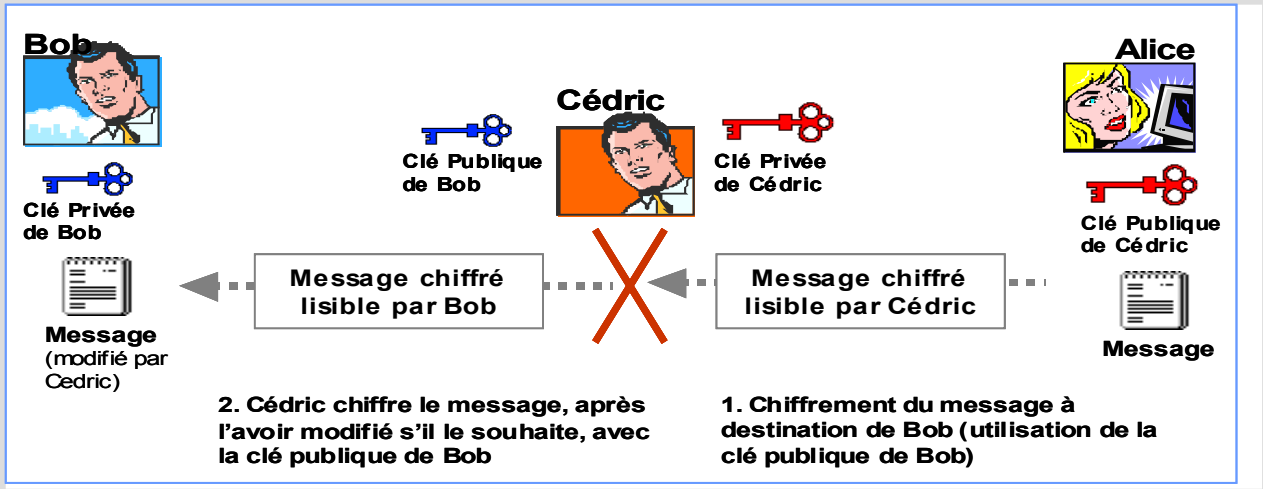
Problème

- Comment être sûr de disposer de la bonne clé publique ?

Il faut disposer d'un intermédiaire de confiance qui détient et distribue les clés publiques.

L'attaque « Man in the middle »





La signature électronique et la notion de certificat

Le problème de la diffusion des clés publiques

Le problème est de s'assurer que la clé que l'on récupére provient bien de la personne concernée : rien ne garantit que la clé est bien celle de l'utilisateur à qui elle est associée.

Un pirate peut **remplacer** la **clé publique** présente dans un annuaire par **sa** clé publique.
Ainsi, il peut déchiffrer tous les messages ayant été chiffrés avec cette clé.
Il peut même ensuite renvoyer à son véritable destinataire le message (modifié ou non) en chiffrant avec la clé originale pour ne pas être démasqué !

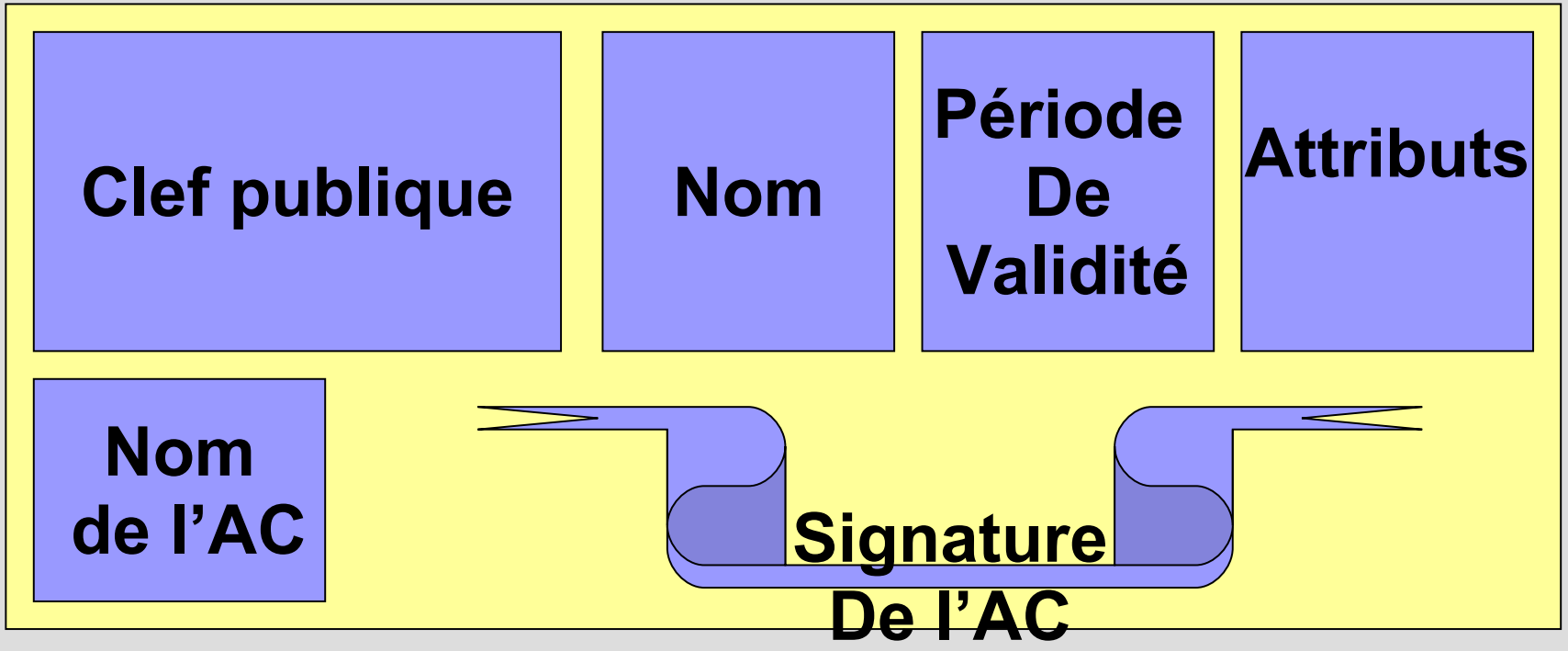
Notion de certificat

Un **certificat** permet **d'associer** une **clé publique** à une **entité** (une personne, une machine, ...) afin d'en assurer la **validité**.
*Le certificat est la carte d'identité de la clé publique, délivré par un organisme appelé **autorité** de **certification**.*
Ces certificats sont émis et signé par une tierce partie, **l'autorité** de **certification** ou CA (Certificate Authority).

L'autorité de certification est chargée de

- **délivrer** les certificats ;
- d'assigner une **date de validité** aux certificats (équivalent à la date limite de péremption des produits alimentaires) ;
- **révoquer** éventuellement des certificats avant cette date en cas de compromission de la clé (ou du propriétaire).

Le certificat établit un lien fort entre le nom (DN) de son titulaire et sa clé publique



Le certificat

Il est construit suivant une norme reconnue internationalement pour faciliter l'interopérabilité.
Un certificat est un petit fichier séparé en **deux parties** :

- une contenant les informations suivantes (norme ISO X509) :
  le nom de l'autorité de certification
  le nom du propriétaire du certificat
  la date de validité du certificat très important, mais pas facile à gérer…
  l'algorithme de chiffrement utilisé
  la clé publique du propriétaire
- une autre contenant la **signature** de **l'autorité** de **certification**

La confiance s'établit en faisant confiance à une **autorité supérieure** : VeriSign, GTE, CommerceNet…

La construction du certificat

L'ensemble des informations (le nom de l'autorité de certification, du propriétaire du certificat…) est **signé** par l'autorité de certification, à l'aide d'un **sceau** :
– une fonction de hachage crée une **empreinte** de ces informations,
– ce résumé est chiffré à l'aide de la **clé privée** de l'autorité de certification, la clé publique ayant été préalablement largement diffusée *ou elle même signée par une autorité de niveau supérieur*.

Grâce à ce sceau, il est possible de s'assurer de la qualité du certificat.

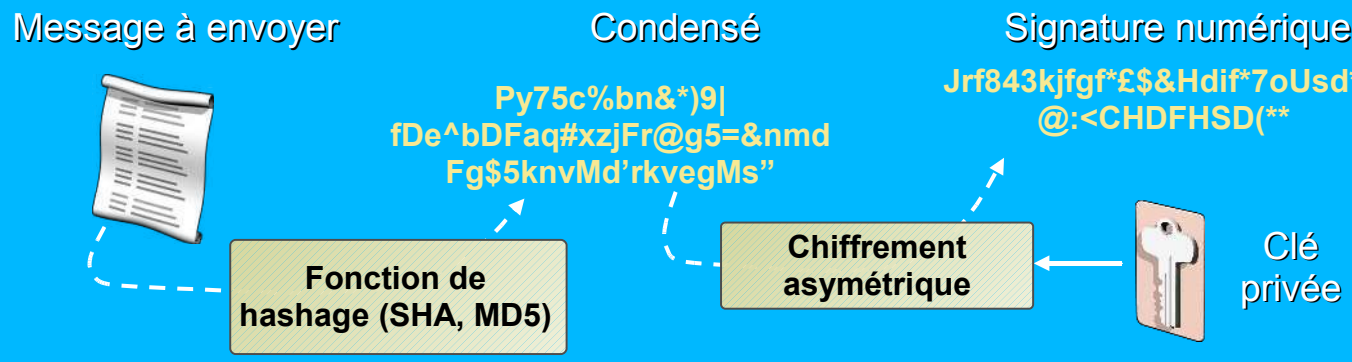
Cette méthode repose sur la **confiance** dans une structure dont on dispose de la clé publique.

Certificats numériques : vérification de la signature

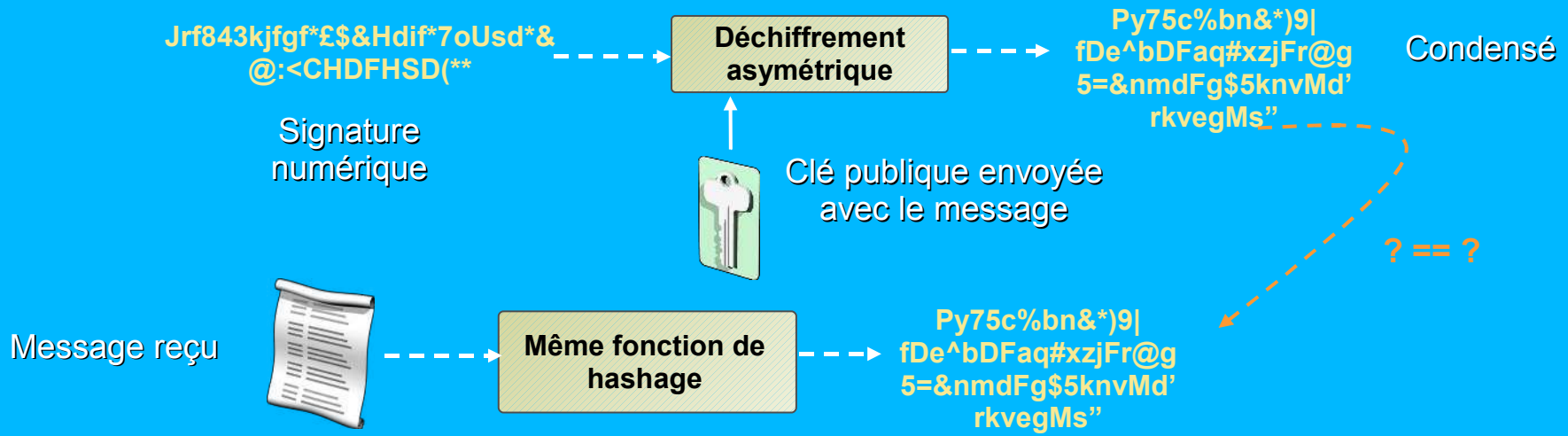
Cryptographie asymétrique (clé publique, clé privée)

Ex. Signature numérique d'un message

Créer une signature numérique (émetteur)

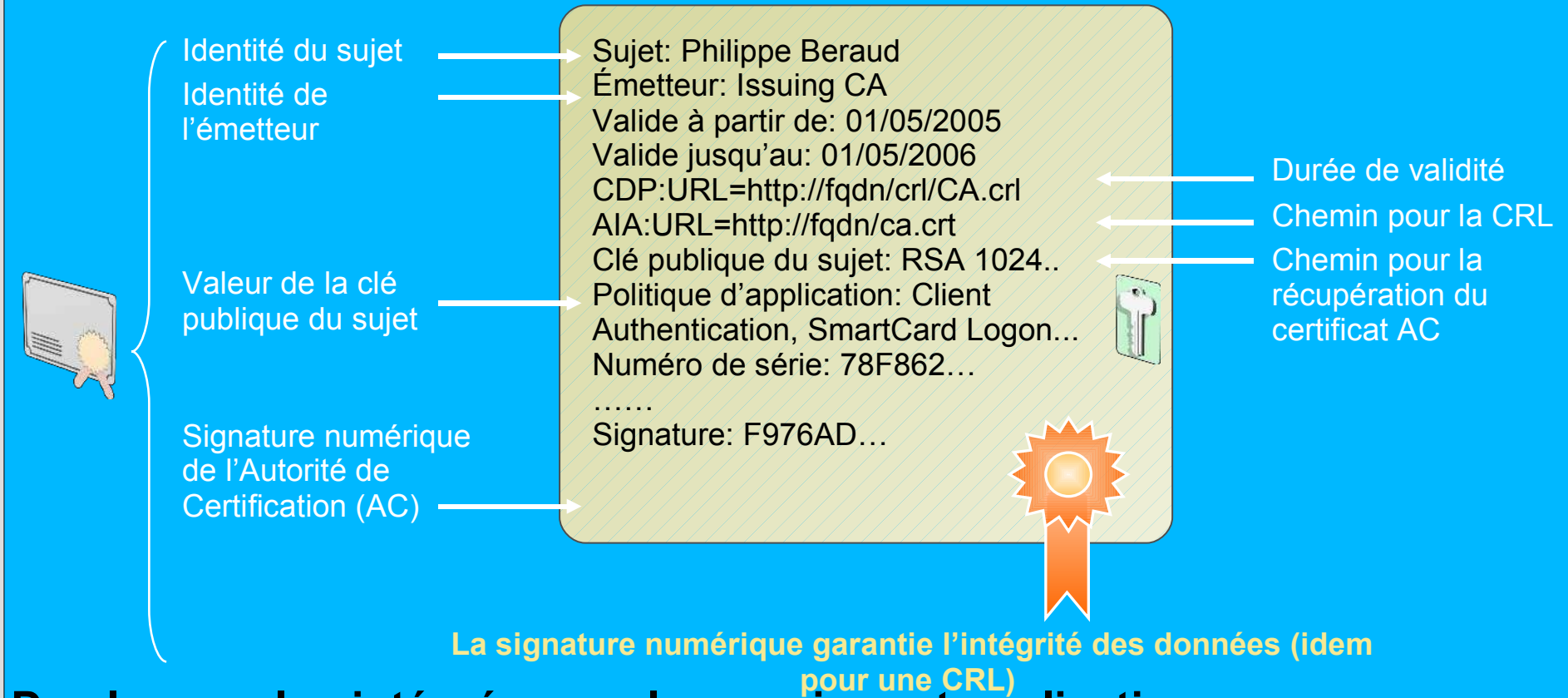


Vérifier une signature numérique (destinataire)



Certificats X509 v3

Équivalent d'une pièce d'identité pour un utilisateur ou une machine



La signature numérique garantie l'intégrité des données (idem pour une CRL)

De plus en plus intégrés avec les services et applications

Ouverture de session par carte à puce, messagerie sécurisée, applications de signature électronique, VPN, WiFi, etc.

Le certificat

Notion de tiers de confiance

Cela consiste à adhérer auprès d'un organisme que l'on appelle autorité de certification.
Cet organisme délivre des certificats.
Cet organisme intègre sa clé publique par exemple au niveau :

- du **navigateur** de la machine dans le cas de la sécurisation d'une transaction web;
- du **système d'exploitation** pour la vérification des mises à jour ou l'installation de logiciel

Notion d'Infrastructure de Gestion de Clef (IGC ou PKI Public Key Infrastructure)

Une Infrastructure de Gestion de Clef est un système assurant la gestion de certificats électroniques au sein d'une communauté d'utilisateurs.
Une IGC est composée

- d'au moins une **autorité** de **certification**,
- d'au moins une **autorité d'enregistrement** chargée :
  - de vérifier les données d'identification des utilisateurs de certificat électronique, et
  - de contrôler les droits liés à l'utilisation des certificats électroniques conformément à la politique de certification.

Une PKI fournit :

- les fonctions de **stockage** de certificats d'un serveur de certificats,
- des fonctions de **gestion** de certificats (émission, **révocation**, stockage, récupération et fiabilité des certificats).

Vérification d'un certificat

- vérifier que le certificat n'a pas expiré, que sa date de validité est correcte ;
- authentifier l'empreinte (provenance de l'AC) et l'intégrité (pas de modification du certificat) ;
- consulter la liste de révocation de l'AC pour savoir s'il n'a pas été révoqué.

Applications

- Applications de confiance (applet JAVA, pilote Windows XP, …)
- Sécurisation des processus « web services » en particulier les serveurs d'authentification (SSO)
- Horodatage
- Signature
- E-commerce
- Dématérialisation de procédure administrative (Workflow)
- E-Vote

Les Usages

- Messagerie S/MIME : signature (certificat de l'émetteur) et/ou chiffrement (certificat du destinataire)
- SSL ou TLS : en particulier HTTPS pour chiffrer les sessions du client et authentifier le serveur. Plus rarement authentifier le client.
  SSL -> POPS, IMAPS, LDAPS, SMTP/TLS, …
- VPN et IPsec

SSL: Secure Socket Layer

Principe :

- utiliser une couche avec chiffrement et authentification au dessus de TCP/IP ;
- implémenter par dessus le protocole de communication (SMTP, POP, HTTP, etc.) ;

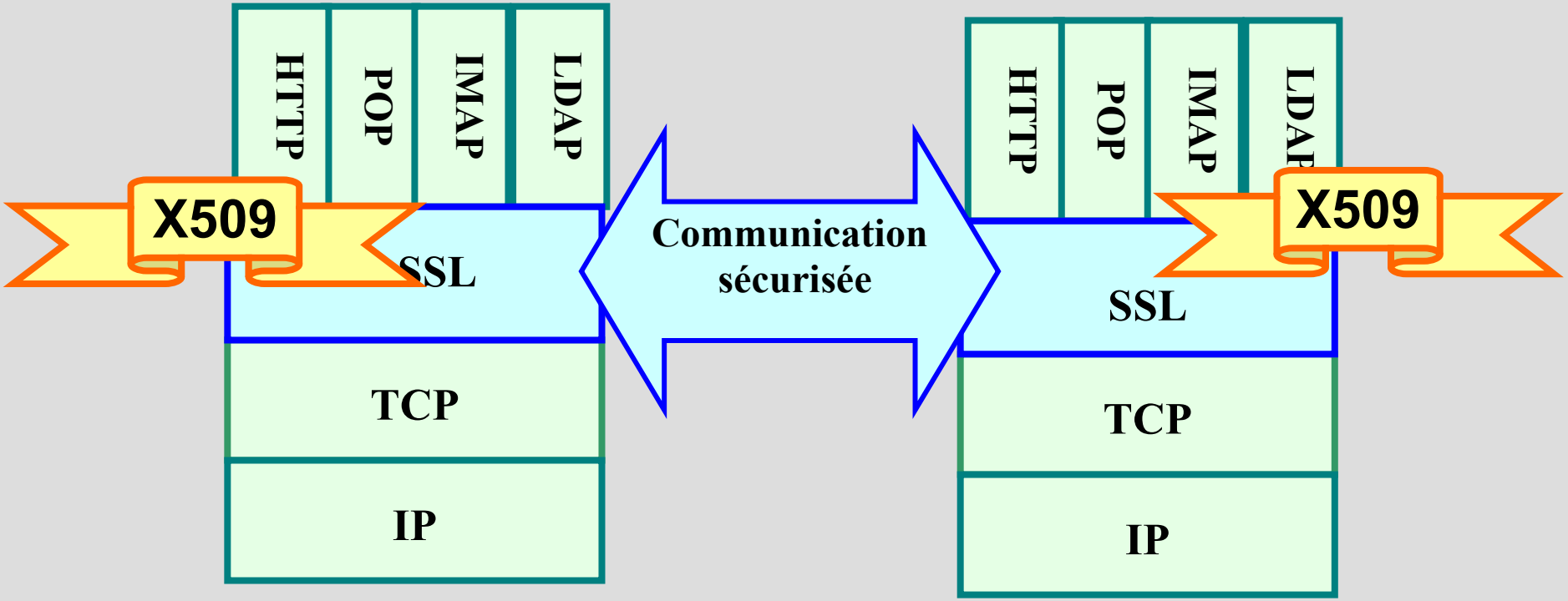
Avantage : Applicable à toutes les applications sur TCP (sans réécriture de celles-ci)

A ce jour, probablement le domaine d'application le plus utilisé (OpenSSL).

Principes généraux de SSL

L'utilisation de SSL permet :

- D'établir un canal de communication chiffré ;
- D'authentifier l'un ou l'autre des interlocuteurs, voire les deux, à l'aide de certificat (au format x509).



La PKI

Le but

Le but de la PKI est de présenter l'autorité de certification, à savoir une entité humaine (une personne, un groupe, un service, une entreprise ou une autre association) autorisée par une société à émettre des certificats à l'attention de ses utilisateurs informatiques.

Une autorité de certification fonctionne comme un service de contrôle des passeports du gouvernement d'un pays.

L'autorité de certification **crée** des **certificats** et les signe de façon numérique à l'aide d'une clé privée qui lui appartient.

Elle gère une **liste** de **révocation** qui permet d'invalider des certificats déja diffusés.

Vérification d'un certificat

On peut vérifier la signature numérique de l'AC émettrice du certificat, à l'aide de la clé publique de l'AC. Si c'est le cas alors il garantit l'intégrité du contenu du certificat (la clé publique et l'identité du détenteur du certificat).

L'utilisation que fait le titulaire du certificat ne concerne plus la PKI, mais les diverses applications qui sont compatibles.

Confiance dans le PKI

L'ensemble des personnes et des services doivent faire confiance à la PKI :

- signature des courriers,
- chiffrement,
- authentification sur des applications maison…

Ils doivent également savoir déchiffrer un certificat et être capable de contacter l´Autorité de Certification afin de vérifier la validité du certificat auprès de la liste de révocation.

La PKI n'est qu'une simple couche destinée à faciliter la gestion des identités numériques à grande échelle.

Elle est totalement indépendante des applications éventuelles qui utilisent ces identités.

La PKI

L'émission de certificat n'est pas le seul service de l'IGC

- vérifie l'identité du titulaire lors de l'émission de certificat
- publie le certificat,
- assure le renouvellement,
- révoque les certificats invalidés,
- assure parfois le recouvrement de la clef privée.

La révocation

Accepteriez vous d'utiliser une carte bancaire si vous ne pouviez par y faire opposition, même en cas de vol ?

Les CRL : la liste des certificats révoqués, liste signée par la CA

Mal implémenté dans les navigateurs

Pas encore de CRL incrémentale.

Alternative : OCSP

La révocation est une limite théorique au modèle des PKIs.

Les composants

On distingue différents composants dans une IGC :

- Autorité de certification AC (certificat authority)
- Autorité d'enregistrement AE (registry authority)
- Interface utilisateur (Enrolment Entity)

Les différentes autorités

L'autorité de certification

C'est une organisation qui délivre des certificats à une population.

Il existe des

- autorités privées (intranet d'une entreprise),
- organisationnelles (CRU, CNRS),
- corporative (notaires),
- commerciales (Thawte, Verisign, …),
- très commerciales (Microsoft),
- institutionnelles, etc

Les tâches de l'AC

- Protège la clé privée de la AC (bunker informatique)
- Vérifie les demandes de certificats (Certificat Signing Request) provenant des AE
- Génère les certificats et les publie
- Génère les listes de certificats révoqués (Certificat Revocation List)

L'autorité d'enregistrement

Vérifie l'identité des demandeurs de certificats et les éléments de la demande.

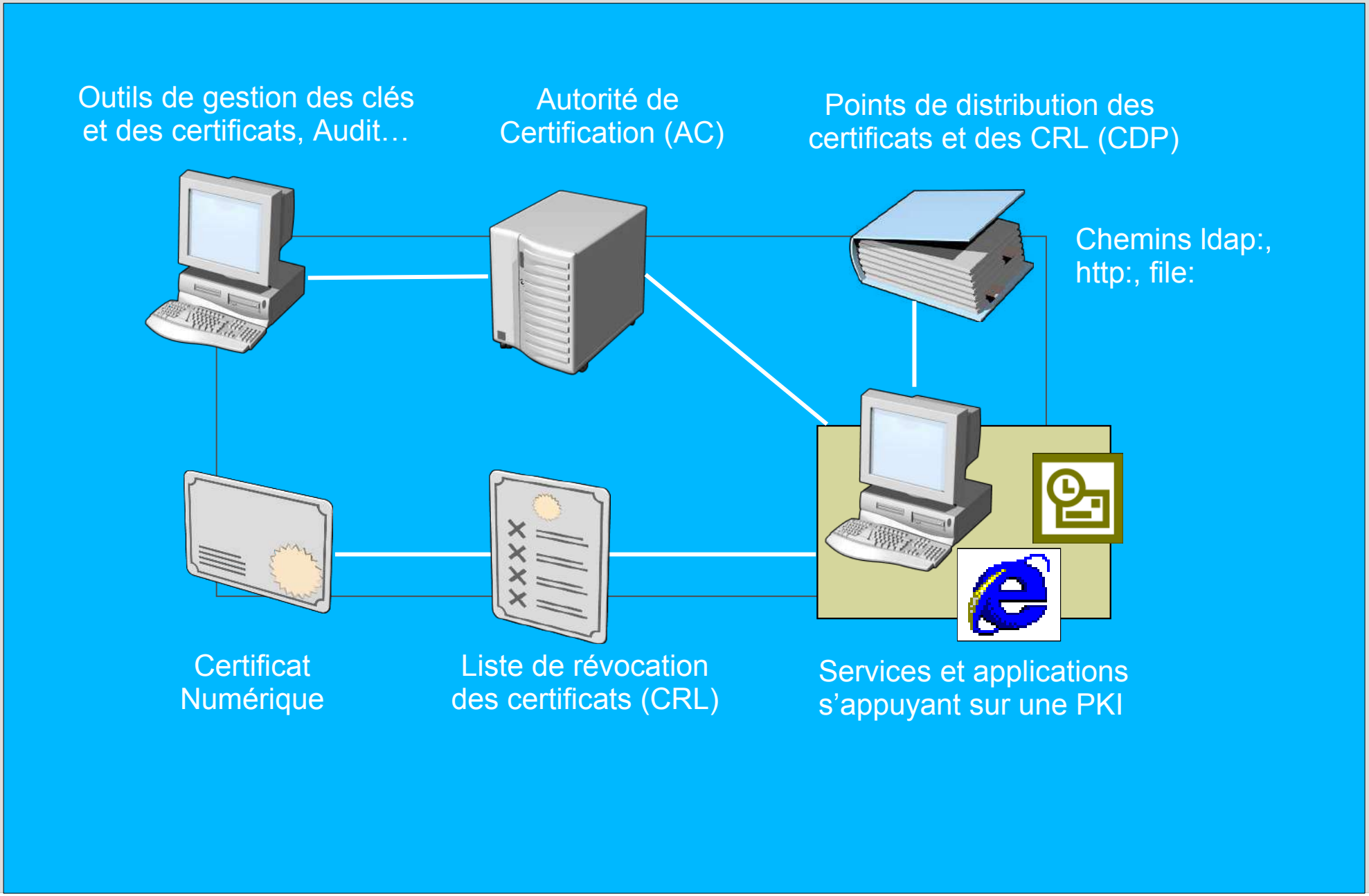
Exemple :

- *L'email présent dans le DN est-il l'email canonique ?*
- *Le demandeur a-t-il le droit de disposer d'un certificat de signature ?*

Transmet les demandes valides par un canal sûr à l'AC (demandes signées par l'opérateur de la AC)

Recueille et vérifie les demandes de révocation

Composants d'une PKI



Les PKI : une rigueur

Un projet ambitieux d'entreprise

Pour une entreprise la démarche est lourde et pas toujours nécessaire :

- pour signer des e-mails ou faire du chiffrement, il existe des méthodes plus légères.
- pour participer à des places de marché, fédérer ses fournisseurs ou ses partenaires, ou unifier les fonctions de signature électronique, alors la PKI est nécessaire au sein de l'entreprise.

Différentes natures de certificat pour une messagerie sécurisée

Il existe plusieurs « classes » de certificat de messagerie en fonction du niveau de confiance demandé.

Des informations d'identité plus ou moins précises sont demandées en fonction du niveau de confiance choisi.

- Classe 1 = une **clé publique** associée à une **adresse email**.
  Le demandeur reçoit automatiquement un mail de confirmation ,
  il n'y a pas de véracité de l'identité du titulaire
  suffisant pour un particulier, service gratuit.

- Classe 2 et supérieure = la vérification des informations d'identité fournies est effectuée,
  la présentation physique peut être nécessaire ;
  Il y aura compensation financière en cas de litige ;
  pour un usage professionnel le certificat de classe 2 ou supérieur est nécessaire.

Les PKIs : les risques

Des problèmes persistent pour l'utilisation de certificat

Lacune du côté technique

La révocation des certificats est basée sur une liste qu'il faut concrètement télécharger régulièrement. Ceci est contraignant et lourd.

Des standards sont en cours d'élaboration pour accéder à cette liste dynamiquement et automatiquement mais ils ne sont pas encore implémentés dans Netscape ou Internet Explorer.

La confiance peut être un danger :

Toute la mécanique de la PKI nécessite des procédures strictes et sérieuses (dans la gestion des certificats…) pour assurer les garanties qui sont affichées.

Mais si les procédures ne sont pas fiables, il y aura des malversations, des faux certificats…

Si ces incidents sont trop nombreux, alors plus personne ne fera confiance aux certificats et ceux-ci n'auront plus aucune valeur.

Ce sera la mort des certificats.

Pas de service public

Tout le secteur est totalement **libéralisé**, il est complètement laissé aux entreprises privées.

Or, celles-ci peuvent avoir tendance à négliger les procédures (coûteuses) pour un profit à court terme.

Des certifications et des vérifications par des organismes gouvernementaux doivent être mis en place dans certains pays, mais pas partout et ils tardent.

Il n'y a par exemple pas encore d'autorité de certification gouvernementale française...

Loi du 13 mars 2000 (Code civil) portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique.

Art. 1316. **-** *La preuve littérale ou preuve par écrit résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification* **intelligible**, *quels que soient leur support et leurs modalités de transmission.*

Art. 1316-1. - *L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment* **identifiée** *la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir* **l'intégrité**.

Art. 1316-2. - *Lorsque la loi n'a pas fixé d'autres principes, et à défaut de* ***convention*** *valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable quel qu'en soit le support.*

Aspects légaux, compléments

Art. 1316-3. **–** *L'écrit sur support électronique a la même force probante que l'écrit sur support papier*

Art. 1316-4. **-** *La signature nécessaire à la perfection d'un acte juridique identifie celui qui l'appose. Elle manifeste le consentement des parties aux obligations qui découlent de cet acte. Quand elle est apposée par un officier public, elle confère l'authenticité à l'acte.*

Alinéa 2 : *Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.*

Exigence d'identification & d'intégrité

Identification de l'auteur, imputabilité de l'acte

Le texte impose à la preuve littérale **l'intégrité** de l'acte dans tout son cycle de vie

La solution:

Signature électronique (cf article 1316-4)

mais:

- Recours à des tiers qualifiés et utilisation de produits répondant à des normes publiées au JOCE du 17 juillet 2003
- Prévoir la possibilité de « re signer » périodiquement

Interprétation pour l'archivage

La loi vise bien la conservation des documents électroniques et impose des exigences :

Intelligibilité: peu importe la forme de l'information, l'essentiel est qu'elle soit restituée de façon intelligible par l'homme et non par la machine

Identification de l'auteur

Garantie **d'intégrité**

Pérennité: respecter les durées de conservation prescrites par les textes, fonction de la nature du document et des délais de prescriptions

L'horodatage

Besoin

Archiver un document pendant un certain temps (obligation légale) ;
Prouver de l'antériorité d'un dépôt de document (le cachet de la Poste faisant foi...)

But

Fournir la preuve de l'existence d'un message à un instant donné

Horodateur neutre / opérations techniques

- Aucun contrôle du contenu du message
- Pas de contrôle du bien fondé de la requête

Contenu du jeton d'horodatage

- Politique d'horodatage utilisée
- Nom du tiers horodateur et son numéro authentification
- Marque de temps
- Empreinte du message à horodater
- Numéro de série unique
- Signature du tiers horodateur
- Diverses autres informations de service

Archivage électronique, scellement

Garantir

- L'intégrité dans le temps
- La pérennité de l'information

Le décret français ne réglemente pas le service d'horodatage

Il y fait toutefois allusion lorsqu'il exige d'un prestataire de certification électronique de :

« veiller à ce que la date et l'heure de délivrance et de révocation d'un certificat électronique puissent être déterminées avec précision. » (Art 6 du décret).

Principe de production