# Sécurité des Systèmes Informations

## Sécurité du courriel

**Ahmed Mehaoua**
**ahmed.mehaoua@parisdescartes.fr**

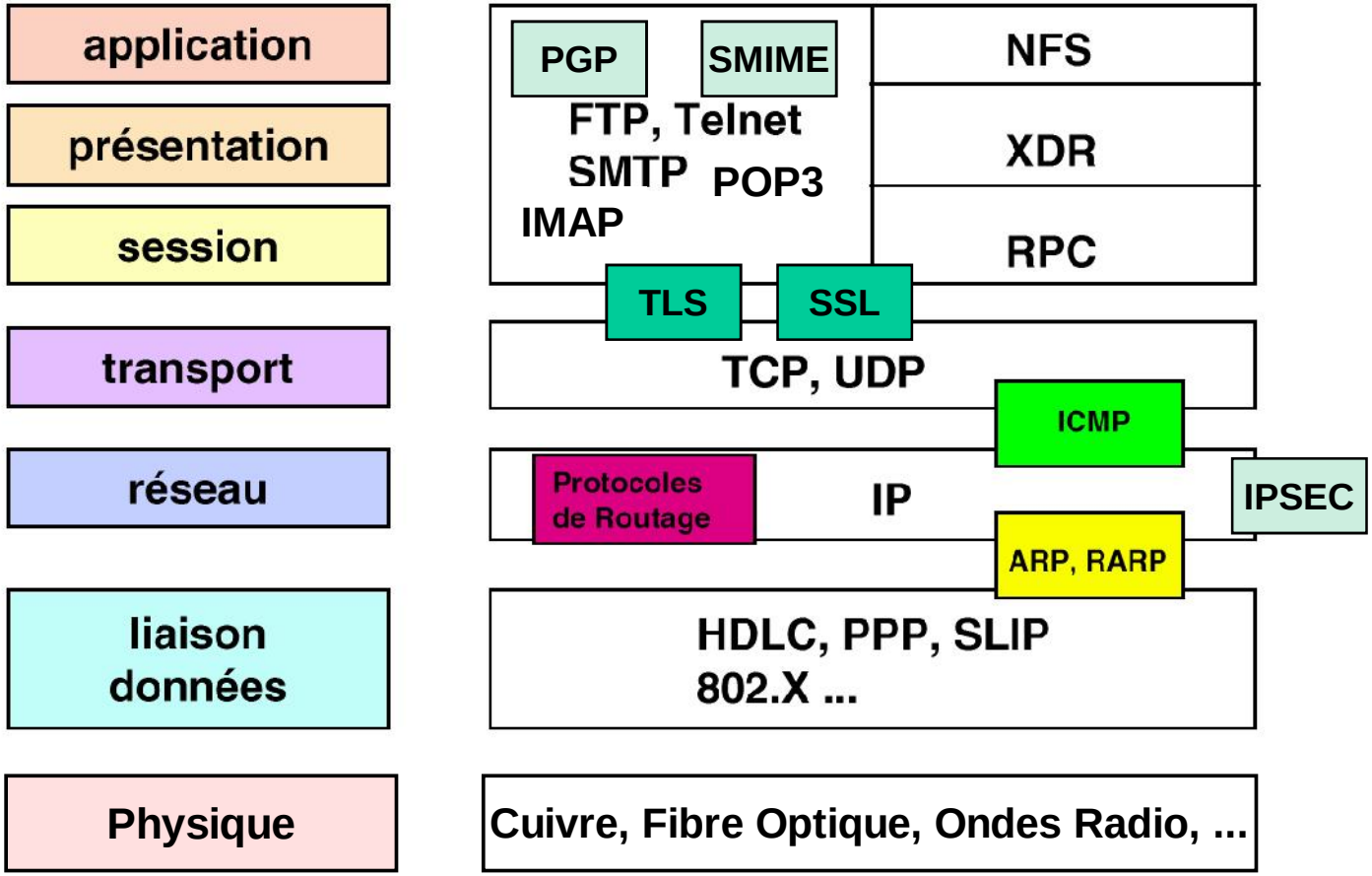
# Plan

1. **Le système de messagerie électronique :**
    1. **WebMail**
    2. **POP3 : Post Office Protocol v3**
    3. **IMAP : Internet Mail Application Protocol**
    4. **SMTP : Simple Mail Transport Protocol**
    5. **MIME : Multipurpose Internet Mail Extension**
2. **La sécurité de la messagerie électronique**
    1. **SSL : Secure Socket Layer**
    2. **PGP : Pretty Good Privacy**
    3. **S/MIME : Secure Multipurpose Internet Mail Extension**

# COURRIER ELECTRONIQUE
## historique

- Le courrier électronique existait avant Internet.
- Le courrier électronique prit forme en 1965 en tant que moyen de communication entre utilisateurs d'ordinateurs à exploitation partagée (time-sharing mainframe).
- le CTSS du MIT a été le premier système de messagerie électronique.
- Dès la création d'ARPANET, en 1969, les premiers programmes de courriel SNDMSG et READMAIL ont joué un rôle important dans le développement du courrier électronique dont ARPANET augmenta de manière significative la popularité.
- En 1972, Ray Tomlinson proposa l'utilisation du signe @ pour séparer les noms d'utilisateur de leur machine.

# SSL/TLS et l'architecture TCP/IP



# WebMail

- Un webmail, anglicisme parfois traduit en courriel Web ou messagerie Web, est une interface web rendant possible l'émission, la consultation et la manipulation de courriers électroniques directement sur le Web depuis un navigateur (HTTP).

- Parmi les moteurs de courrielleurs web connus, on trouve : IMP/HORDE, RoundCube, SquirrelMail (webmail en php).

- IMP (Internet Messaging Program) est une application PHP sous licence GPL permettant de consulter sa messagerie électronique au travers d'une interface Web. IMP utilise les protocoles IMAP et POP3 pour accéder à la messagerie.

# RECEPTION DES MESSAGES
# Protocole POP3

- POP3, ou Post Office Protocol Version 3 (littéralement le protocole du bureau de poste, version 3), est un protocole qui permet de récupérer les courriers électroniques situés sur un serveur de messagerie électronique.
- Cette opération nécessite une connexion à un réseau TCP/IP. Le port serveur utilisé est le 110.
- Ce protocole a été défini dans la RFC 1939.
- POP3S (POP3 over SSL) utilise SSL pour sécuriser la communication avec le serveur, tel que décrit dans la RFC 2595. POP3S utilise le port 995.

# RECEPTION DES MESSAGES
# Protocole IMAP4

- IMAP4, ou Internet Mail Access Protocol Version 4, est un protocole qui permet de gérer interactivement les courriers électroniques situés sur un serveur de messagerie électronique.
- Cette opération nécessite une connexion à un réseau TCP/IP. Le port serveur utilisé est le 143.
- Ce protocole a été défini dans la RFC 3531.
- IMAPS (IMAP over SSL) utilise SSL pour sécuriser la communication avec le serveur, tel que décrit dans la RFC 2595. POP3S utilise le port 993.

# RECEPTION DES MESSAGES
# POP3 vs IMAP4

- Les paradigmes hors ligne et en ligne reflètent deux modes distincts d'utilisation :
  - ✓ **Hors ligne** = récupération à la demande vers une machine cliente unique.
  - ✓ **En ligne** = accès interactif à de multiples boîtes aux lettres depuis plusieurs clients.
- Avantages du paradigme hors ligne :
  - ✓ Temps de connexion minimal.
  - ✓ Utilisation minimale des ressources du serveur.
- Avantages du paradigme en ligne :
  - ✓ Possibilité d'utiliser différents ordinateurs à différents instants.
  - ✓ Accès à de multiples boîtes aux lettres indépendamment de la plate-forme.
  - ✓ Possibilité d'accès concurrentiel à des boîtes aux lettres partagées.

# TRANSFERT DES MESSAGES
# Protocole SMTP

- Le Simple Mail Transfer Protocol (littéralement « Protocole simple de transfert de courrier »), généralement abrégé SMTP, est un protocole de communication utilisé pour transférer le courrier électronique vers les serveurs de messagerie électronique.
- Définit dans le RFC 2821.  Utilise TCP port 25.
- SMTP over SSL (SMTPS) utilise TCP port 465
- Comme le protocole utilisait du texte en ASCII (7 bits), il ne fonctionnait pas pour l'envoi de n'importe quels octets dans des fichiers binaires. Pour pallier ce problème, des standards comme MIME ont été développés pour permettre le codage des fichiers binaires au travers de SMTP.

# TRANSFERT DES MESSAGES SMTP

- Un enregistrement Mail eXchanger (MX) est un type d'enregistrements du Domain Name System qui associe un nom de domaine à une liste ordonnée de serveurs de messagerie électronique.
- Le serveur d'envoi va consulter le DNS pour obtenir la liste des enregistrements MX associés au domaine de destination, et tenter de contacter le serveur dont la priorité est la plus faible, et s'il n'y arrive pas, tenter de contacter le second, et ainsi de suite.
- nslookup –type=MX parisdescartes.fr

# COURRIER ELECTRONIQUE

## Format des messages RFC2822

**Assez ancien => pas de distinction nette entre l'enveloppe et l'en-tête**

***En-tête :***

***To :***
***Cc :***
***Bcc :***
***From :***

***Sender :***
***Received :***
***Return Path :***

**1 ligne « Received » est ajoutée par chaque agent de transfert de message (nom, date, heure ...)**

**Quelques champs sont ajoutés :**
**Date ; Reply-to ; Message-Id ; In-Reply-to ; Subject**

**Possibilité de créer ses propres champs d'en-tête**

# FORMATS DES MESSAGES MIME

- MIME, ou Multipurpose Internet Message Extensions, est une spécification décrivant les formats de messages multimédias sur l'Internet.

- MIME permet en particulier :
  - l'échange de textes écrits dans des jeux de caractères autres que l'anglais (chinois, russe, arabe, …),
  - l'échange de pieces jointes multimédia (image, vidéo, audio, pdf, doc, xls …).

- MIME : est définit dans RFC 1341, mis à jour RFC 1521

# Email sécurisé

- **Comment échanger des emails sécurisé ?**
  - **Protection contre : capture, modification, rejeu, etc.**
- **Si l'émetteur et le récepteur partagent une clé secrète !**
  - **facile, mais comment peut-on partager une clé avec un inconnu ?**

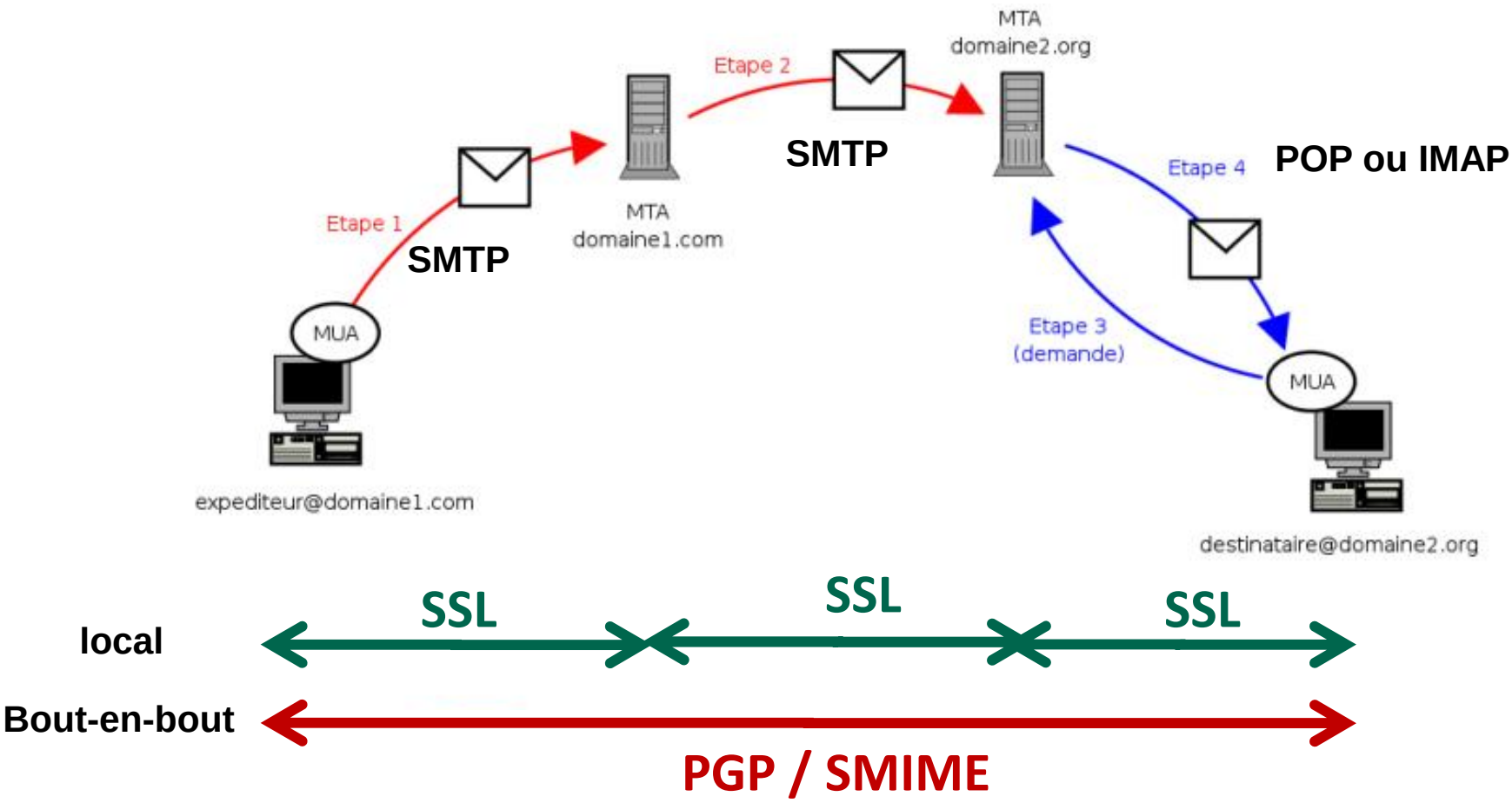
# Email sécurisé

- Le chiffrement à clé publique permet de distribuer une clé secrète (pour le chiffrement symétrique)
  - Car le chiffrement symétrique est 1000 fois plus rapide que le chiffrement asymétrique
  - Mais on ne veut pas payer pour un certificat personnel issue d'une autorité de certification (AC) pour échanger des emails !!!!
- La solution est d'utiliser PGP ou S-MIME

# Email et sécurité
# - de bout en bout -

- Il existe deux principaux systèmes pour crypter les mails de bout-en-bout, qui ont une origine et une philosophie très différente.
  - S/MIME (Secure MIME) : solution héritée du monde du commerce électronique, développé et soutenu par les industriels du secteur.
  - PGP (Pretty Good Privacy) : solution à destination des particuliers et développé par un informaticien américain Zimmermann.

# Securité du Courriel



# Sécurisation des échanges

**Pour sécuriser les échanges d'emails ayant lieu sur le réseau Internet, il existe plusieurs approches :**

1. **avec PGP ou S-MIME, au niveau de la couche application (intégré au client email)**
2. **avec TLS/SSL vise à sécuriser les échanges au niveau de la couche Transport (Internet) ou Session/Présentation (modèle OSI).**

# PGP

- Pretty Good Privacy
- PGP est un système de chiffrement
  - Basé sur les mécanismes de cryptographie existants
  - RSA, IDEA, CAST, DES, MD5, SHA1, etc.
- créé initialement par Philip Zimmermann, un analyste informaticien pour permettre le respect de la vie privée dans les correspondances par courrier électronique.

- Il est très rapide et sûr
- Contrairement au modèle S/MIME , PGP ne nécessite pas de Tiers de Confiance, mais fonctionne sur un principe décentralisé, le Réseau de Confiance (Web of Trust).

# PGP : Services de sécurité

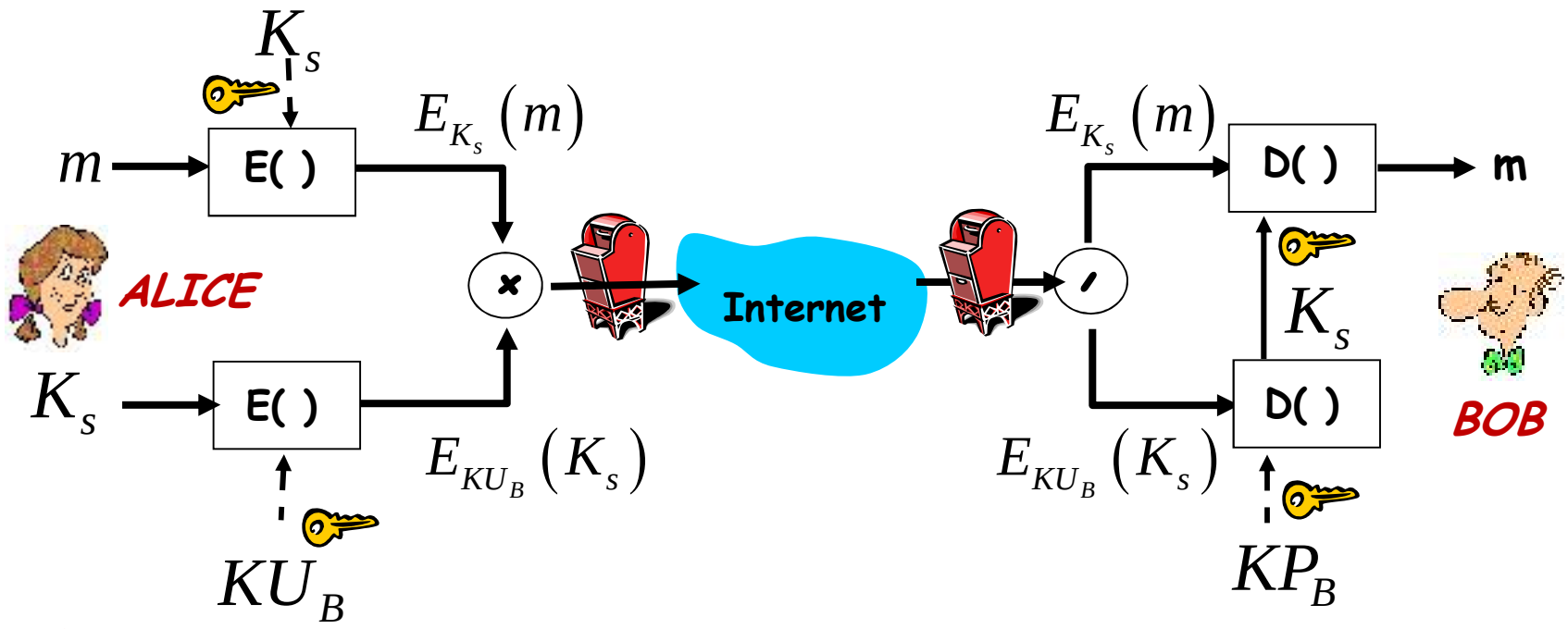
- Signature électronique et vérification d'intégrité de messages : fonction basée sur l'emploi simultané d'une fonction de hachage (MD5) et du système RSA. MD5 hache le message et fournit un résultat de 128 bits qui est ensuite chiffré, grâce à RSA, par la clef privée de l'expéditeur.
- Chiffrement des fichiers locaux : fonction utilisant IDEA.
- Génération de clefs publiques et privées : chaque utilisateur chiffre ses messages à l'aide de clefs privées IDEA. Le transfert de clefs électroniques IDEA utilise le système RSA; PGP offre donc des mécanismes de génération de clefs adaptés à ce système. La taille des clefs RSA est proposée suivant plusieurs niveaux de sécurité : 512, 768, 1024 ou 1280 bits.

# PGP : Services de sécurité

- Gestion des clefs : fonction s'assurant de distribuer la clef publique de l'utilisateur aux correspondants qui souhaiteraient lui envoyer des messages chiffrés.
- Certification de clefs : cette fonction permet d'ajouter un sceau numérique garantissant l'authenticité des clefs publiques. Il s'agit d'une originalité de PGP, qui base sa confiance sur une notion de proximité sociale plutôt que sur celle d'autorité centrale de certification.
- Révocation, désactivation, enregistrement de clefs : fonction qui permet de produire des certificats de révocation publiable sur des serveurs publiques.

# PGP: Confidentialité

- Alice veut envoyer un email confidentiel e-mail à Bob

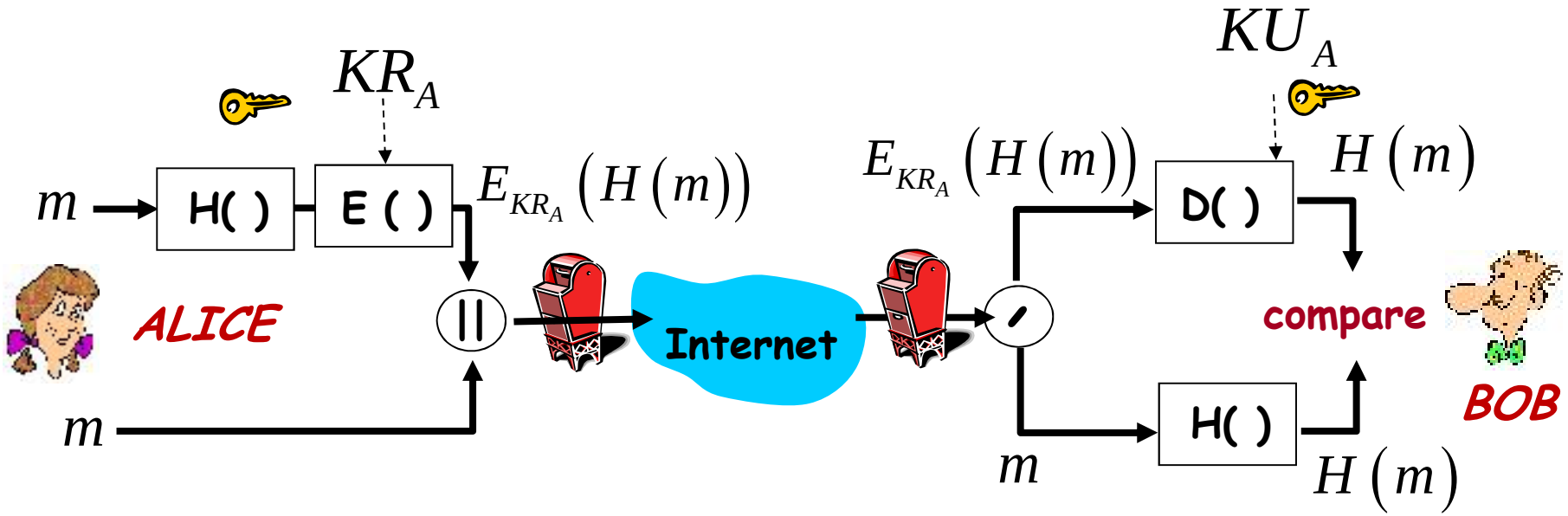



**Alice:**

- génération d'une clé symétrique (random) : $K_S$
- chiffrement du message *m* avec $K_S$ (chiffrement symétrique)
- chiffrement de la clé $K_S$ avec la clé publique de Bob (chiff. Asymétrique)
- Transmission à Bob du message chiffré: $E_{KS}(m)$ & la clé chiffrée $E_{KUB}(K_S)$.

# PGP: Authentification & intégrité

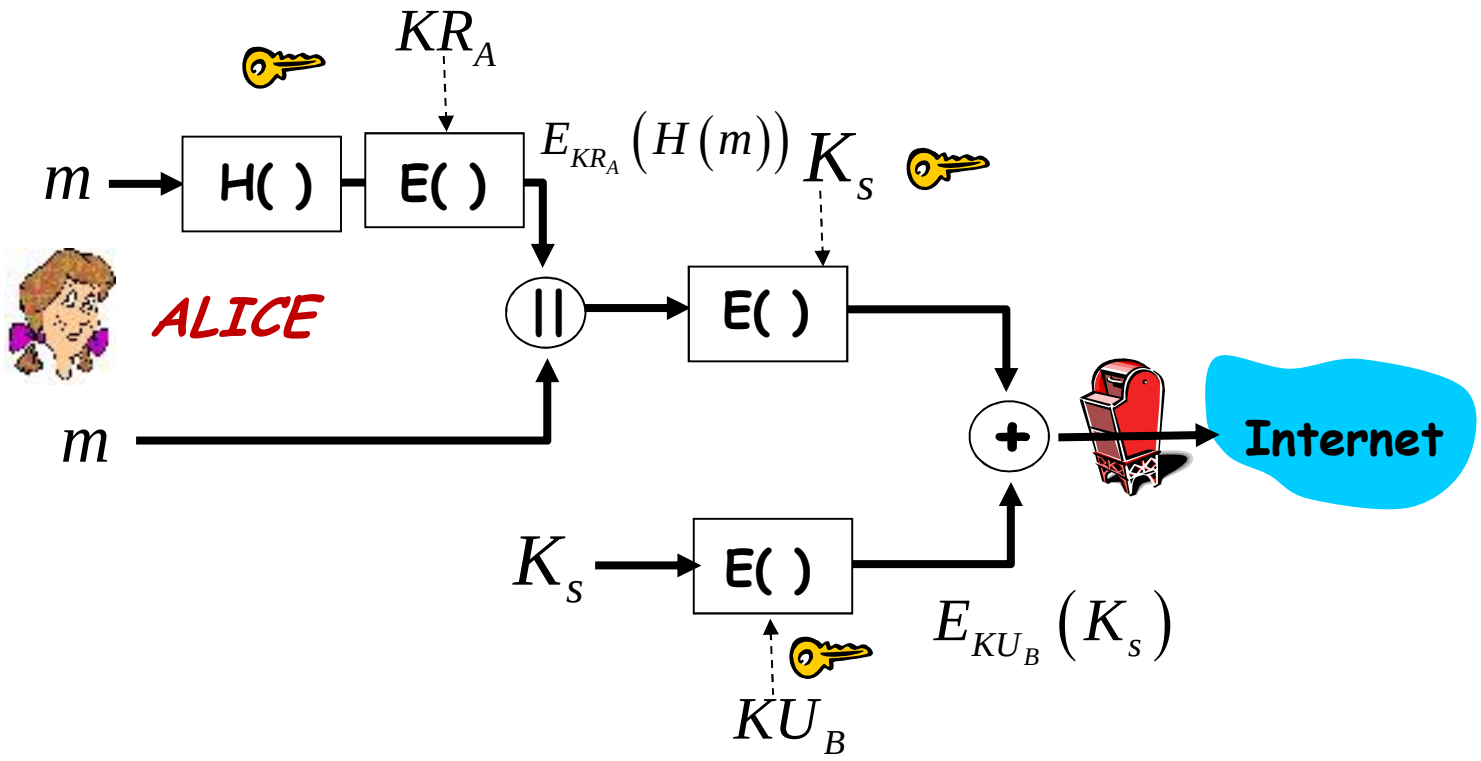
- Alice *signe* son message




- Alice envoi le message en claire et sa signature à Bob

# Confidentialité & authentification & intégrité

- Alice veut envoyer un message avec les services de sécurité:
  - Confidentialité, authentification, intégrité




- **Alice Utilise 3 clés :** sa clé privé, la clé publique de bob, la clé symétrique crée

# PGP : fonctionnement

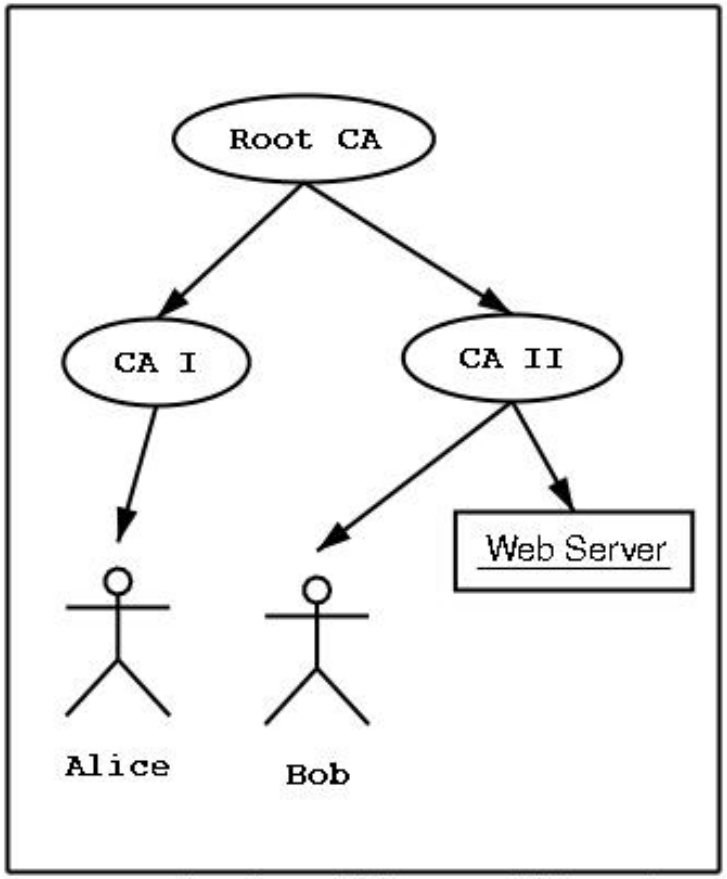
- Compression : le texte à envoyer est compressé. Cette étape permet de réduire le temps de transmission des données, et améliore également la sécurité. En effet, la compression détruit les modèles du texte (fréquences des lettres, mots répétés). Et on sait que ces modèles sont souvent utilisés dans les analyses cryptographiques.
- Chiffrement du message : une clé de session aléatoire est générée, et le message est chiffré par un algorithme symétrique à l'aide d'une clé de session. L'algorithme utilisé a varié au cours du temps : il s'agissait au début d'IDEA, puis de CAST et 3DES.
- Chiffrement de la clé de session : la clé de session est chiffrée en utilisant la clé publique du destinataire (et l'algorithme RSA).
- Envoi et réception du message : l'expéditeur envoie le couple message chiffré / clé de session chiffrée au Destinataire. Celui récupère d'abord la clé de session, en utilisant sa clé privée, puis il déchiffre le message grâce à la clé de session.

# PGP : certificat

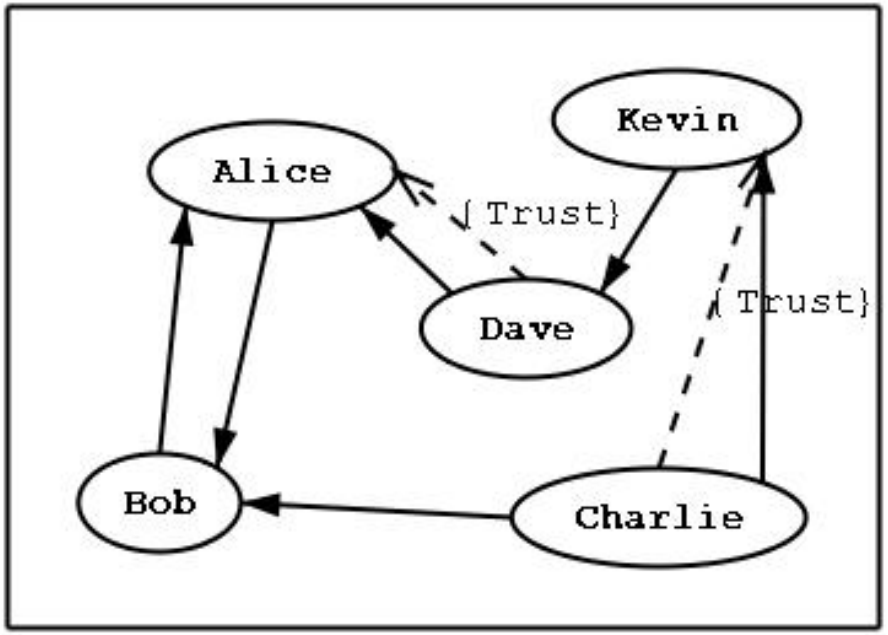
Un certificat PGP comprend, entre autres, les informations suivantes :

1. Le numéro de version de PGP : identifie la version de PGP utilisée pour créer la clef associée au certificat.
2. La clef publique du détenteur du certificat : partie publique de votre paire de clefs associée à l'algorithme de la clef, qu'il soit RSA, DH ou DSA.
3. Les informations du détenteur du certificat : il s'agit des informations portant sur l'« identité » de l'utilisateur, telles que son nom, son ID utilisateur, sa photographie, etc.
4. La signature numérique du détenteur du certificat : également appelée *autosignature*, il s'agit de la signature effectuée avec la clef privée correspondant à la clef publique associée au certificat.
5. La période de validité du certificat : dates/ heures de début et d'expiration du certificat. Indique la date d'expiration du certificat.
6. L'algorithme de chiffrement symétrique préféré pour la clef : indique l'algorithme de chiffrement que le détenteur du certificat préfère appliquer au cryptage des informations. Les algorithmes pris en charge :CAST, IDEA ou 3DES

# PGP : Web of Trust & Keyservers




Two typical X.509 Certification paths




An example of the web of trust model

# S-MIME

- S/MIME a été développé initialement par RSA Data Security
- S/MIME (Secure/Multipurpose Internet Mail Extensions) propose un moyen d'envoyer et de recevoir des messages « sécurisés ».

- S/MIME est basé sur le standard MIME et fournis les services cryptographiques suivants :
  1. authentification
  2. intégrité du message
  3. non répudiation (signature)
  4. chiffrement (confidentialité).


- S/MIME n'est pas uniquement destiné au mail, il peut être utilisé par tout mécanisme qui transporte des données MIME

# S-MIME

- S/MIME n'effectue pas une signature, S/MIME défini comment créer un message MIME avec des services cryptographiques (chiffrement et signature).
- La signature est basés sur PKCS #7 et S/MIME utilise les types de données définis dans PKCS #7.

| Fonctionalités requises | S/MIME v3 |
|---|---|
| Format de message | Binary, based on CMS |
| Format de certificat | Binary, based on X.509v3 |
| Algorithme de cryptage symétrique | TripleDES (DES EDE3 CBC) |
| Algorithme de signature | Diffie-Hellman (X9.42) with DSS |
| Cryptage de clés | RSA |
| Algorithm de hash | SHA-1 |
| Encapsulation MIME de données signées | Choice of multipart/signed or CMS format |
| Encapsulation MIME de données cryptées | application/pkcs7-mime |

# S/MIME vs OpenPGP

| Mandatory features | S/MIME v3 | OpenPGP |
|---|---|---|
| **Message format** | Binary, based on CMS | Binary, based on previous PGP |
| **Certificate format** | Binary, based on X.509v3 | Binary, based on previous PGP |
| **Symmetric encryption algorithm** | TripleDES (DES EDE3 CBC) | TripleDES (DES EDE3 Eccentric CFB) |
| **Signature algorithm** | Diffie-Hellman (X9.42) with DSS or RSA | ElGamal with DSS |
| **Hash algorithm** | SHA-1 | SHA-1 |
| **MIME encapsulation of signed data** | Choice of multipart/signed or CMS format | multipart/signed with ASCII armor |
| **MIME encapsulation of encrypted data** | application/pkcs7-mime | multipart/encrypted |

# PGP vs S/MIME

- Dans le cadre de la correspondance entre personnes privées, les arguments de décentralisation et d'indépendance de PGP en font un système de choix, pour peu que leurs utilisateurs respectent les règles du "réseau de confiance".
- S/MIME est plus intéressant pour des sociétés, ou pour le commerce électronique. Le coût élevé d'une Autorité de Certification se justifiant par le risque financier pour les protagonistes. Ces derniers préfèrent payer leur dime plutôt que de risquer de se faire "arnaquer".

# Travaux Pratiques

- Etape 1 : installation et configuration d'un système de courrier électronique.
  - Partie Serveur
  - Partie Client
- Etape 2 : analyse des protocoles POP3 et SMTP.
  - Utilisation du sniffer de réseau Wireshark
  - Capture du login et du mot de passe en claires
  - Capture du contenu d'un courriel
- Etape 3 : sécurisation du courriel avec GnuPG
  - Sur les postes clients avec Enigma (PGP)
- Etape 4 : sécurisation des communications émails avec SSL
  - Envoi sécurisé des courriels avec SMTP over SSL (SMTPS)
  - Réception sécurisé des courriels avec POP3 over SSL (POP3S)

# Travaux pratiques