Année 2008-2009

esil

Sécurité des systèmes informatiques
— utilisation de la cryptographie —

Nicolas Baudru
mél : nicolas.baudru@esil.univmed.fr
page web : nicolas.baudru.esil.perso.univmed.fr

Services de sécurité

esil

☞ L'ISO a défini 6 services de sécurité :

- authentification (de la source et/ou du destinataire) ;
- contrôle d'accès (qui nécessite une authentification préliminaire) ;
- confidentialité des données (les données illicitement récupérées doivent être inutilisables) ;
- intégrité des données (empêcher les modifications des données, les doublons) ;
- non-répudiation (un message, son envoi et sa réception ne peuvent être contestés) ;
- protection de l'analyse du trafic (la relation entre deux personnes doit rester secrète).

☞ Différents mécanismes tels que le chiffrement, les signatures numériques, les listes de contrôle d'accès, le bourrage, la notarisation, etc, sont utilisés pour assurer ces services.

Place du chiffrement

esil

☞ Le mécanisme de chiffrement existe à trois niveaux :

- liaison : mise en place de boîtes noires sur les supports de transmission ;
- réseau : des équipements spécialisés sont placés sur chacun des sites, au niveau des routeurs ;
- de bout en bout : seules les données constituant l'information transmise sont chiffrées. Il est mis en oeuvre dans les applications du modèle TCP/IP.

☞ L'ensemble repose, dans tous les cas, sur un algorithme donné, une clé ou un couple de clés associées et un mécanisme de distribution des clés.

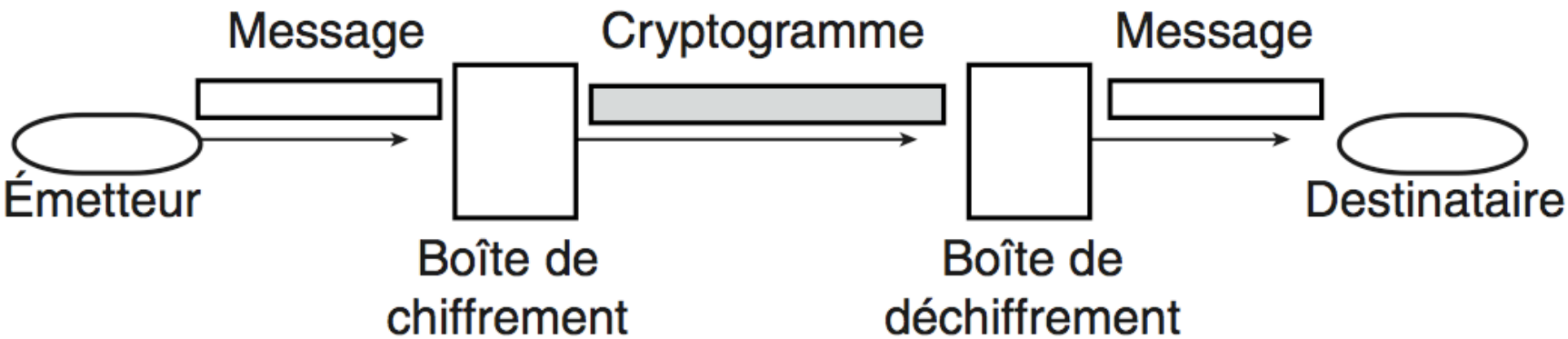
Plan

esil

Plan

esil

Modèle de chiffrement



Vocabulaire

esil

- Chiffrer : transcrire, à l'aide d'un algorithme paramétrable un message clair en une suite incompréhensible de symboles
- texte en clair : le message à chiffrer
- texte chiffré : le résultat du chiffrement
- Déchiffrer : retrouver le texte en clair à partir du texte chiffré à l'aide d'un algorithme paramétrable
- clé : le paramètre des algorithmes de chiffrement et de déchiffrement
- Décrypter : retrouver le texte en clair à partir du texte chiffré sans la clé
- Cryptographie : science du chiffrement
- Cryptanalyse : science du décryptage
- Cryptologie : cryptographie et cryptanalyse
- Cryptosystème : ensemble des méthodes de chiffrement et de déchiffrement utilisables en sécurité

Remarque : le verbe "crypter" n'est pas utilisé.

Notation

esil

- Chiffrement d'un texte en clair P au moyen de la clé K_1 :

$$C = E_{K_1}(P)$$

- Déchiffrement du texte chiffré C au moyen de la clé K_2 :

$$P = D_{K_2}(C)$$

- Si D_{K_2} et la fonction inverse de E_{K_1}, nous obtenons :

$$D_{K_2}[E_{K_1}(P)] = P$$

Propriétés des cryptosystèmes

esil

☞ Les algorithmes de chiffrement et de déchiffrement doivent permettre d'atteindre des vitesses de chiffrement élevés et utiliser peu d'espace mémoire.

☞ Le chiffre doit être difficile à casser que ce soit avec des messages chiffrés seuls ou un échantillon de messages en clair avec leur message chiffré correspondant.

☞ Redondance : le destinataire doit pouvoir vérifier la légitimité d'un message : on ne doit pas pouvoir créer des textes "ressemblant" à des textes chiffrés.

☞ Fraîcheur : le destinataire doit pouvoir s'assurer qu'un message est récent.

Principe de Kerckhoff

esil

☞ Principe de Kerckhoff :

tous les algorithmes doivent être publics ; seules les clés sont secrètes.

☞ Conséquences :

- le véritable secret réside dans la clé ;
- l'algorithme public doit être fort et la clé doit être longue.

☞ Problèmes :

- quelle longueur de clés choisir ?
- quelle fréquence de renouvellement des clés choisir ?
- comment s'échanger les clés ?

Plan

Méthodes de chiffrement

esil

☞ Chiffres de substitution Chaque lettre ou groupre de lettres est remplacé par une autre lettre ou un autre groupe de lettres.
Exemple : avec la clé
texte en clair : 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
texte chiffré : U X O M P S N B E A Z Q W D G V K H C R T Y I F J L
le message “hello world” devient “BPQQG IGHQM”.

☞ Chiffres de transposition On modifie l’ordre des lettres d’un texte en clair.
Exemple : avec la clé 213 le message “hello word” devient “eolhlolwd”.

2	1	3
h	e	l
l	o	w
o	l	d

☞ La plupart des algorithmes de chiffrement ne sont qu’un mélange savant de substitutions et transpositions (ex : DES, AES).

Masques jetables (one time pad)

esil

Technique ancienne permettant de construire des chiffres incassables :

- on choisit un masque (une suite de bits) aléatoire : c'est la clé ;
- on convertit le texte en clair en une chaîne de bits (suivant le code ASCII par exemple) ;
- on effectue un OU exclusif (XOR) entre ces deux chaînes de bits.

Le texte chiffré ne peut être cassé car dans un texte assez long, les lettres apparaîssent avec la même fréquence : le texte chiffré ne contient aucune information.

Algorithmes à clé symétrique

esil

☞ La même clé sert pour le chiffrement et le déchiffrement

☞ Principaux algorithmes connus :

Chiffre	Auteur	Lg. de clé	Commentaires
DES	IBM	56 bits	trop faible
IDEA	Massey et Xuejia	128	efficace mais breveté
RC5	Ronald Rivest	128 à 256	efficace mais breveté
Rijndael	Daemen et Rijmen	128 à 256	meilleur choix
Serpent	Anderson, Biham, Knudsen	128 à 256	très bon
Triple DES	IBM	168	second meilleur choix
Twofish	Bruce Schneier	128 à 256	très bon et très utilisé

☞ Faiblesses :

- La distribution des clés restent un des problèmes majeurs ;
- Certaines méthodes de cryptanalyse diiférentielle et/ou linéaire permettent d'attaquer plus "efficacement" les chiffrements par bloc comme DES.

Algorithmes à clé publique

esil

☞ Caractéristique :

- la clé de chiffrement K_1 et la clé de déchiffrement K_2 sont différentes ;
- Il est difficile de déduire D_{K_2} à partir de E_{K_1} ;
- E_{K_1} ne peut pas être cassé à l'aide d'une attaque sur un texte clair choisi.

☞ Supposons qu'Alice veuille envoyer à Bob un message secret :

1. Bob rend son algorithme de chiffrement paramétré par sa clé public (noté E_{B_1}), et garde son algorithme de déchiffrement paramétré par sa clé (différente de la première) secret (noté D_{B_2}) ;
2. Alice envoie un message P à Bob en le chiffrant à l'aide de E_{B_1} ;
3. Bob reçoit le message chiffré E_{B_1} et le déchiffre avec D_{B_2} (qu'il est le seul à connaître) ;

☞ Principal algorithme connu RSA (de Rivest, Shamir et Adelman) :

- résiste depuis un quart de siècle ;
- utilise une clé de 1024 bits => temps de calcul trop important ;
  ➥ principalement utilisé pour distribuer des clés de session pour AES ou DES.

Plan

Obtenir la confidentialité

esil

- Avec de la cryptographie à clé privée :

- Avec de la cryptographie à clé public :

Obtenir l'intégrité (d'un message seul)

esil

- ☞ Avec de la cryptographie à clé privée :

- ☞ Avec de la cryptographie à clé public :

Obtenir l'intégrité (dans un flot de données)

Obtenir l'authentification d'un message

esil

- Avec de la cryptographie à clé privée :

- Avec de la cryptographie à clé public :

Plan

Signature

esil

☞ But : La signature numérique est une méthode permettant de signer des textes d'une façon qui les mettent à l'abri de toute falsification (comme pour les signatures apposées à la main).

☞ Il faut donc un mécanisme qui permette d'envoyer des messages signés remplissant les conditions suivantes :

- le destinataire peut authentifier l'identité de l'expéditeur ;
- l'expéditeur ne peut pas répudier le contenu de son message ;
- le destinataire (ou un tiers) ne peut pas falsifier le message signé.

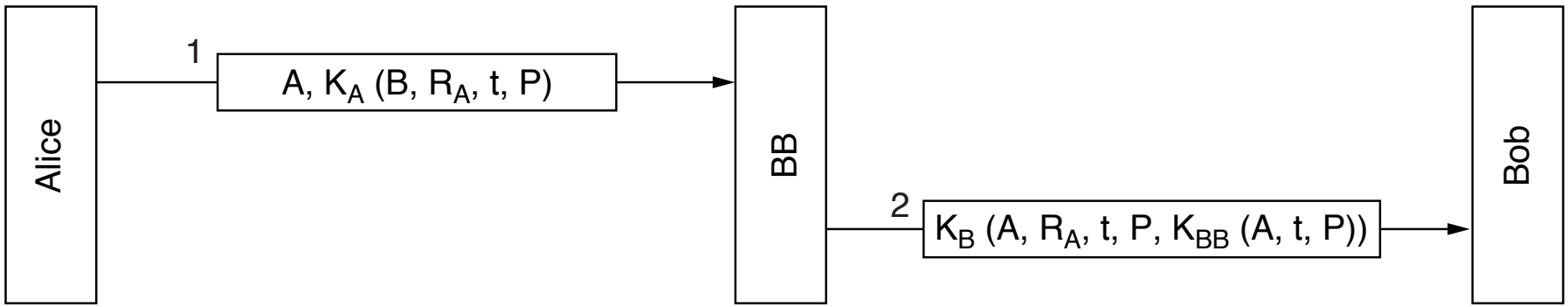
☞ Deux catégories de réponses :

- La responsabilité totale du secret des clés ;
- La notarisation.

Signature à clé symétrique

esil

☞ Utilisation d'un notaire BB en qui tout le monde a confiance.

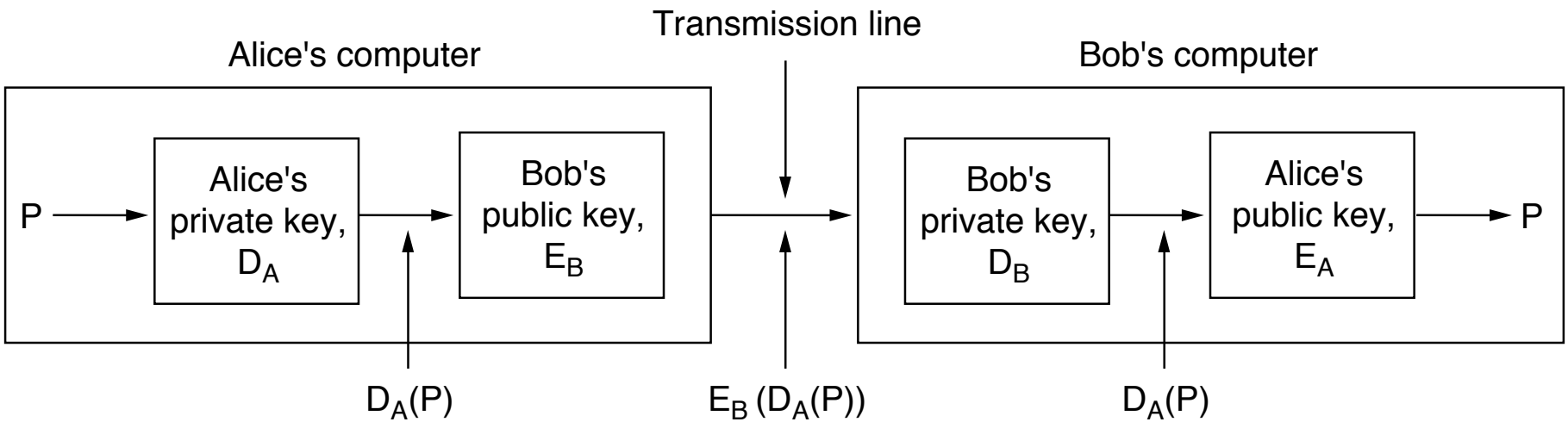


- K_A : clé secrète d'Alice et BB
- K_b : clé secrète de Bob et BB
- R_A : nombre aléatoire
- t : une horodate

Signature à clé publique

☞ On suppose ici que les algorithmes de chiffrement et déchiffrement commutent :

$$E[D(P)] = P = D[E(P)]$$



☞ Cette méthode fonctionne tant que les clés demeurent secrètes

☞ On utilise en général RSA ou DSS.

Condensats de messages

esil

☞ Repose sur un schéma de hachage capable de transformer un texte en clair P de longueur arbitraire en une chaîne de bits MD(P) de longueur fixe, et tel que :

- pour tout P, MD(P) est facile à calculer
- quelque soit MD(P), il est impossible de retrouver P
- pour tout P, personne ne peut trouver un P' tel que MD(P') = MD(P)
  ➥ le hachage doit avoir une longueur > 128 bits
- toute modification de P produit un résultat très différent

☞ On utilise en général MD5 ou SHA-1.

Plan

Le problème

esil

☞ Comment font deux entités A et B pour s'échanger leur clés publiques s'ils ne se connaissent pas ?

Quelques exemples de méthodes :

- première méthode : les clés publiques sont diffusées via leur site web.
  ➥ Ne fonctionne pas, les clés peuvent être falsifiées...
- deuxième méthode : faire appel à un centre de distribution des clés.
  ➥ Que se passe-t-il en cas de panne ? En cas de surcharge ?
- Utiliser une organisation de certification pour certifier que les clés appartiennent bien à leurs légitimes propriétaires.
  ➥ C'est la méthode choisie. Repose sur la création de certificat.

Certificats

esil

☞ Rôle :

- Créer un lien entre une clé publique et le nom de son détenteur.
- Créer un lien entre un clé publique et un attribut (l'age du détenteur par ex.).

☞ Modèle d'un certificat :

Nom :	Durand
Prénom :	Jean
Clé publique :	A6739EC9379...BED3787B
:	
CA :	CNRS
Date de validité :	du 12/02/2007 au 24/12/2007
Empreinte digitale :	213CC...E23B

L'empreinte digitale est un condensat du message signé avec la clé privée du CA.

☞ Les certificats ne sont ni secrets, ni protégés.

X.509

esil

☞ Afin de simplifier la gestion et la validation des certificats, ceux-ci ont été standardisés : norme X.509 de UIT (et RFC 3280 de IETF).

☞ Cette norme est simplement une façon de décrire des certificats. Les principaux champs d'un certificat sont :

Champs	Signification
Version	Version de X.509 utilisée
Numéro de série	Identifiant unique du certificat
Algo de signature	Algo utilisé pour signer le certificat
Emetteur	Nom du CA
Période de validité	
Nom du sujet	Personne dont la clé est certifiée
Clé publique	Clé publique du sujet et identité de l'algo qui l'utilise
Extensions	
Signature	Signature du certificat avec la clé publique du CA

X.509 – Exemple

PKIs

esil

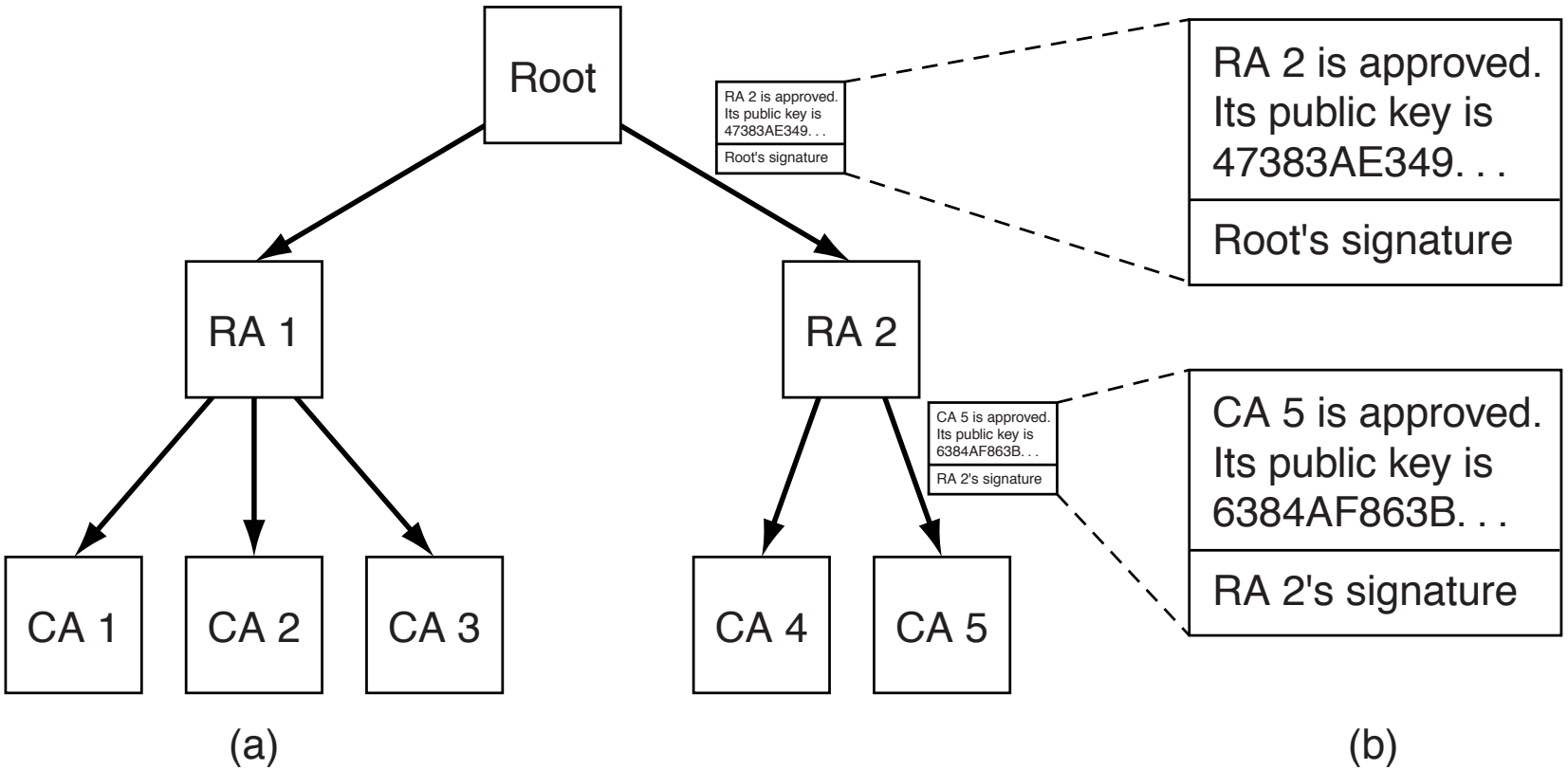
☞ PKI : infrastructures à clés publiques. une PKI fournit un moyen de structurer ses composants et de définir des standards pour différents documents et protocoles.

☞ Une PKI regroupe :

- les utilisateurs
- les CAs organisées de manière hiérarchique
- les certificats
- les annuaires
- les certificat revocation lists (CRL)

Hiérarchie des CAs

esil



☞ Une chaîne de certificats remontant jusqu'au CA root est appelée une chaîne de confiance ou chemin de certification.

Problématique des PKIs

esil

☞ en pratique il y a plusieurs CAs root, appelés ancres de confiance (trust anchors), chacune d'elles administrant ses propres CA, RA, CRLs...

☞ Une partie de ces ancres sont stockées dans les navigateurs selon une politique propre à l'éditeur.
➥ il faut faire confiance à l'éditeur du navigateur...

☞ Où stocker les certificats (et les chaînes de certification) ?

- chez chaque utilisateur ?
- utiliser les DNSs comme annuaires de certification ?
- utiliser des serveurs spécialisés du type LDAP ?

☞ Comment révoquer un certificat ?

Plan

esil

La problèmatique

esil

☞ L'authentification consiste à vérifier que, lors de l'établissement d'une communication, la personne "à l'autre bout du fil" est bien celle qu'elle est supposée être.

☞ Remarque : authentification $\neq$ autorisation

➥ avant d'autoriser quelqu'un à faire quelque chose il faut l'authentifier.

☞ Schéma général d'un protocole de communication lorsque Alice veut communiquer avec Bob :

- Alice commence par envoyer des messages soit à Bob, soit à un KDC (Key Distribution Center) afin de s'authentifier et de convenir d'une clé secrète de session.
- Cette clé de session sera ensuite utilisée dans les échanges qui vont suivre.
- A la fin de l'échange la clé de session est jetée.

La problèmatique

esil

☞ Pourquoi utiliser une clé de session ?

- pour limiter la quantité de texte chiffré que pourrait intercepter un intrus.
- pour limiter les dommages qui pourraient résulter du crash d'un processus et d'un vidage mémoire.
- l'authentification et la confidentialité sont facilement obtenus à l'aide de clés publiques...
  ... mais en pratique, le chiffrement utilisé lors des échanges est réalisé avec un algorithme du type triple DES ou AES, plus rapide que les algorithmes de chiffrement utilisant des clés publiques.

☞ Dans ce qui suit on supposera toujours qu'un intrus, Eve, peut intercepter, modifier ou rejouer certains messages afin de tromper Alice ou Bob.

Authentification fondée sur une clé secrète partagée

esil

☞ On suppose ici que Alice et Bob partagent déjà une clé secrète K_{AB}.

☞ Les trois premiers protocoles que nous allons étudier sont appelés protocoles question-réponse.

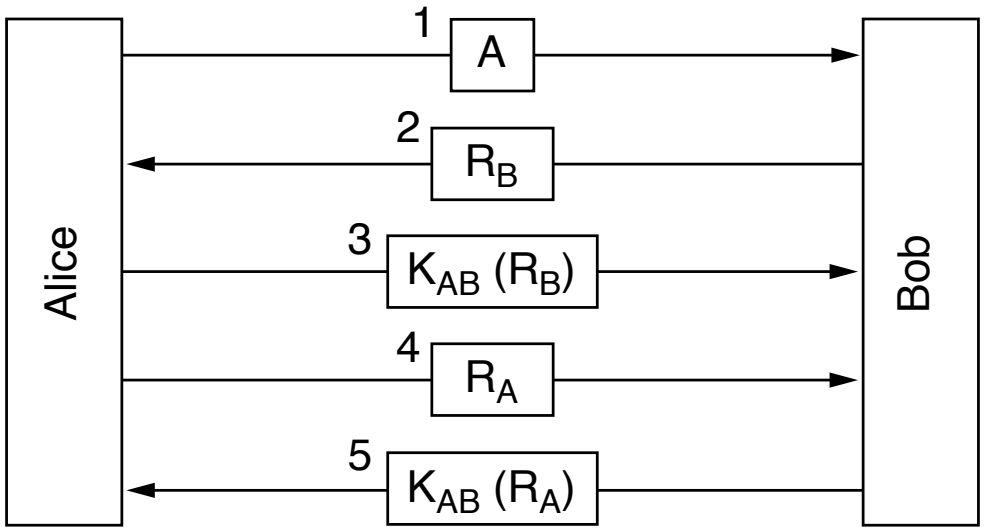
☞ Notation :

- A : Alice ; B : Bob
- R_i : nombre aléatoire (la question) choisi par $i \in \{A, B\}$
- K_i est la clé de $i \in \{A, B\}$
- K_s est la clé de session

Authentification fondée sur une clé secrète partagée

esil

☞ Un premier protocole question-réponse en 5 temps :

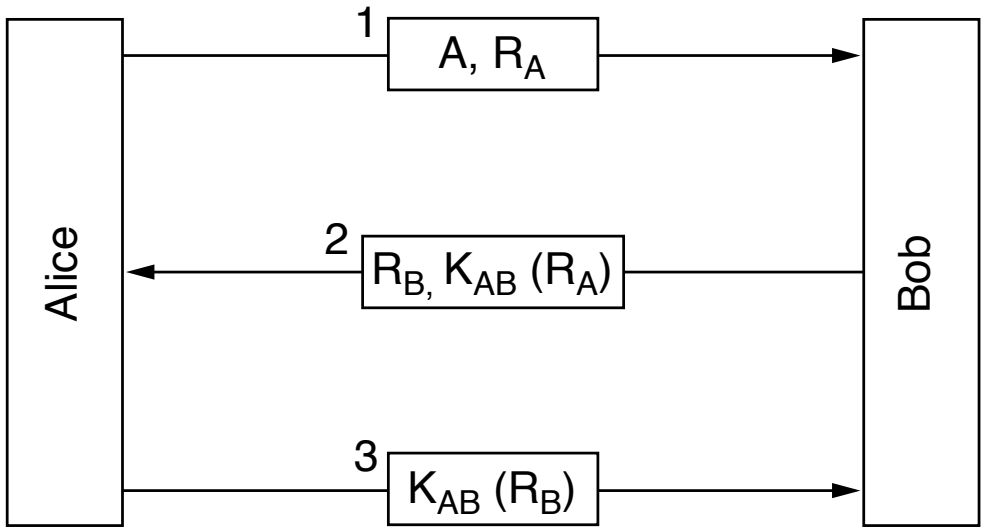


Est-il correct ?

Authentification fondée sur une clé secrète partagée

esil

☞ Un second protocole question-réponse en 3 temps :

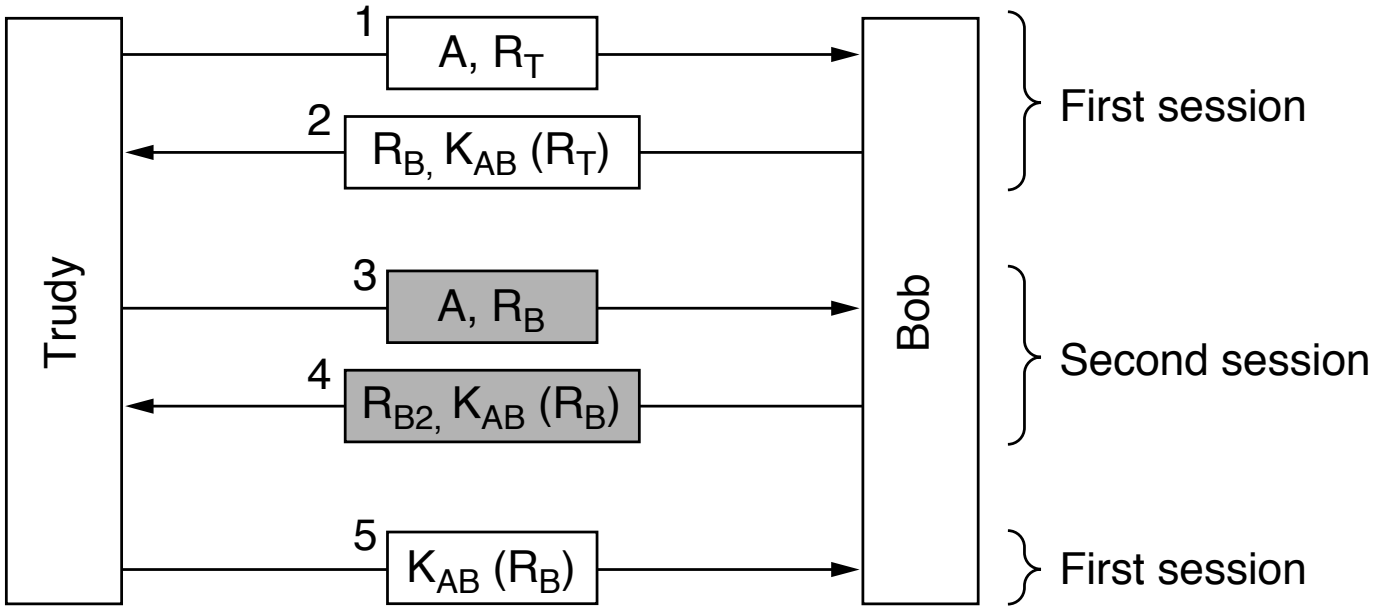


Est-il correct ?

Authentification fondée sur une clé secrète partagée

esil

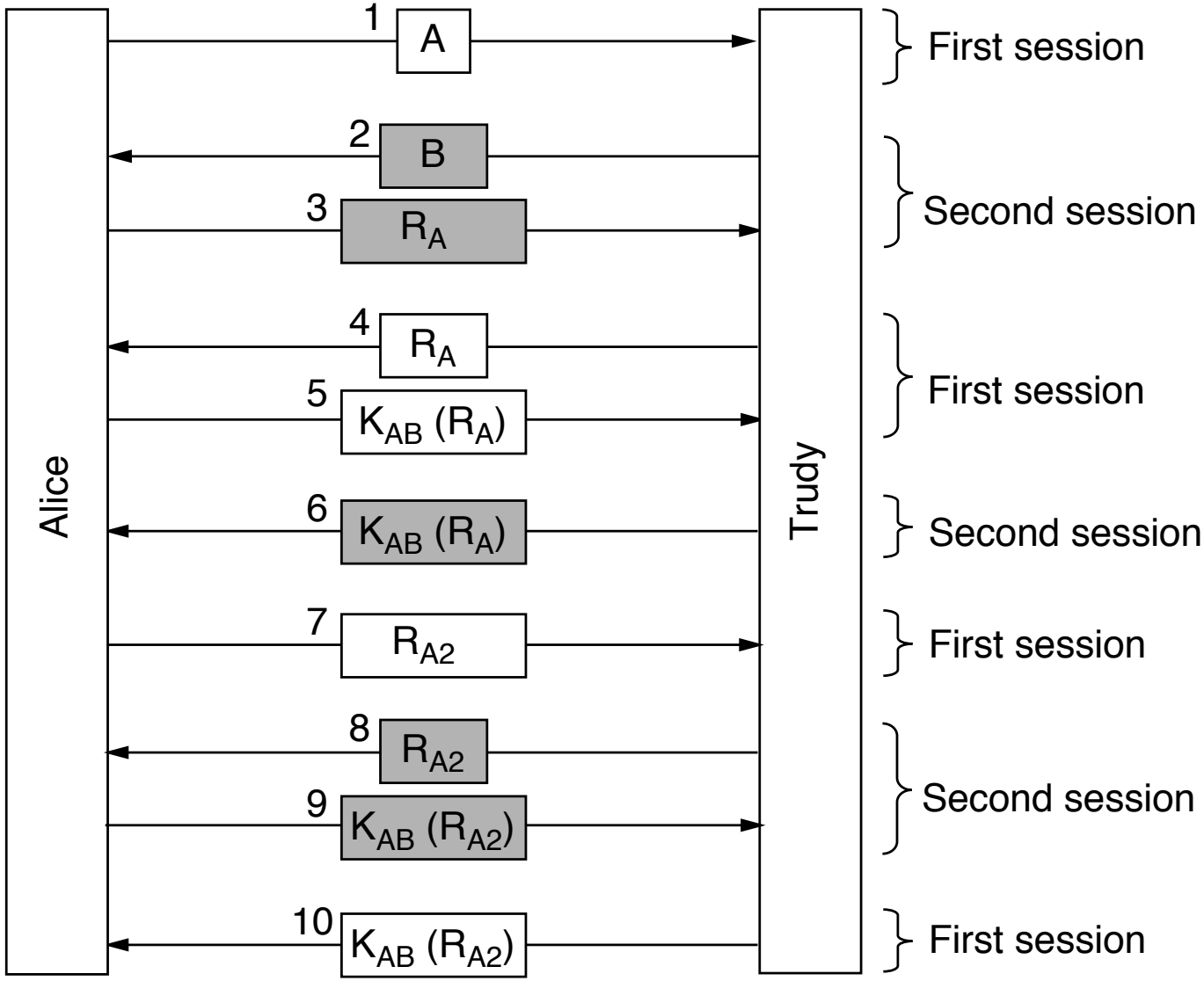
☞ Attaque par réflexion du protocole question-réponse en 3 temps :



Authentification fondée sur une clé secrète partagée

esil

☞ Attaque par réflexion du protocole question-réponse en 5 temps :



Authentification fondée sur une clé secrète partagée

esil

☞ Quatre règles importantes :

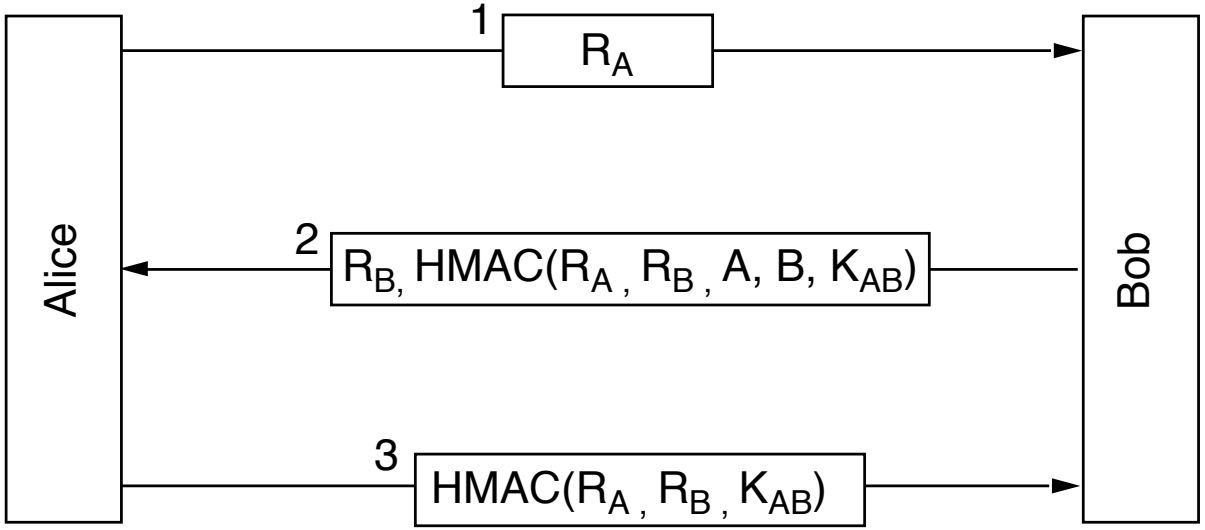
1. l'initiateur du dialogue doit prouver son identité avant son interlocuteur
2. les deux parties doivent utiliser des clés différentes
3. les deux parties doivent choisir leurs questions dans des ensembles différents
4. le protocole doit résister aux attaques utilisant deux sessions

☞ Si l'une de ces règles n'est pas respectée, alors il y a de forte chance que le protocole puisse être cassé.

Authentification fondée sur une clé secrète partagée

esil

☞ Enfin un protocole question-réponse correct !



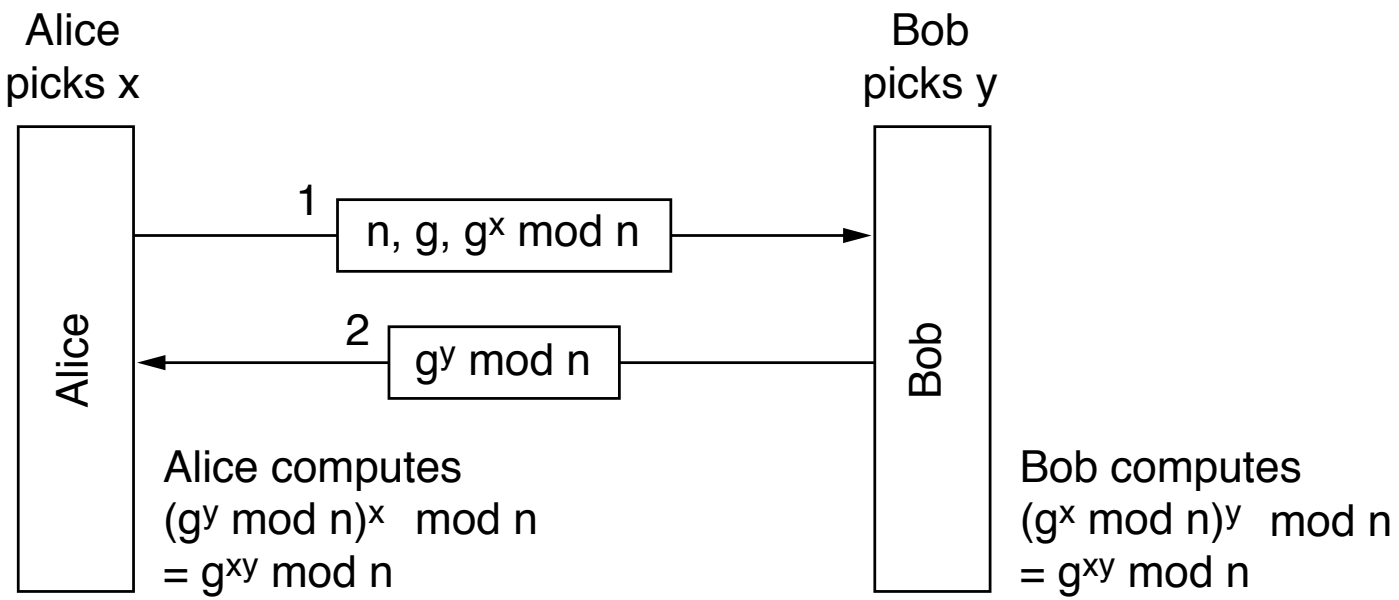
Etablissement d'une clé partagée

esil

☞ On suppose maintenant qu'Alice et Bob ne partagent pas de clé secrète

☞ Pour choisir une clé secrète :

1. Alice et Bob vont se mettre d'accord sur deux grands nombres n et g tels que n et $(n-1)/2$ soient premiers entre eux et g remplisse certaines conditions.
2. Alice et Bob exécutent le protocole de Diffie-Hellman, avec x et y très grands :

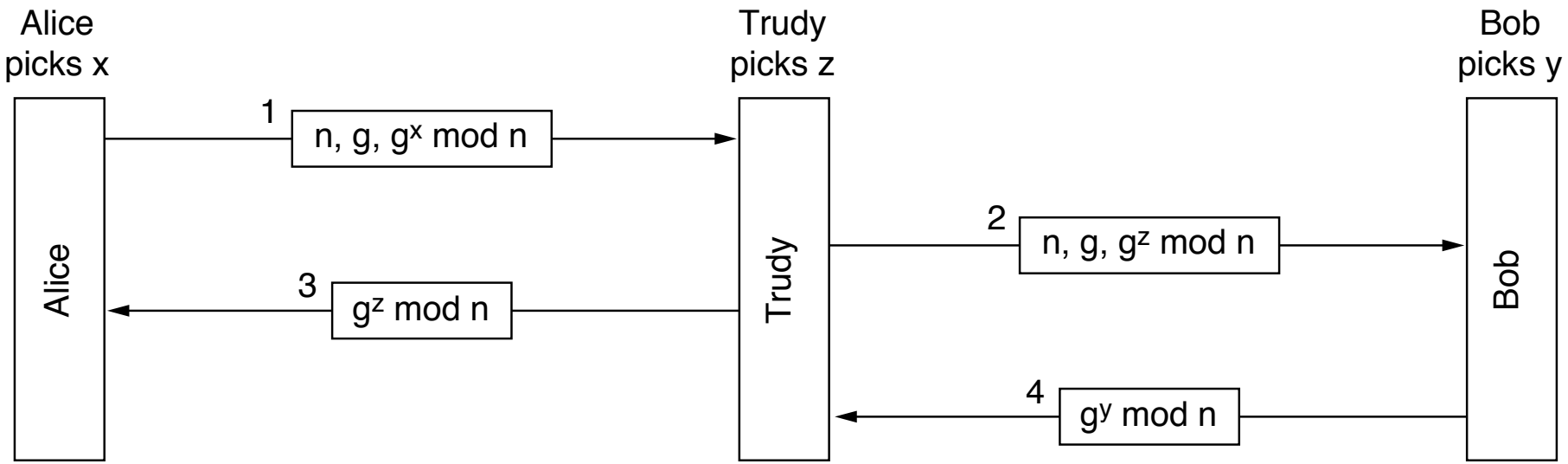


Cela fonctionne-t-il ?

Etablissement d'une clé partagée

esil

☞ L'attaque "man in the middle" :



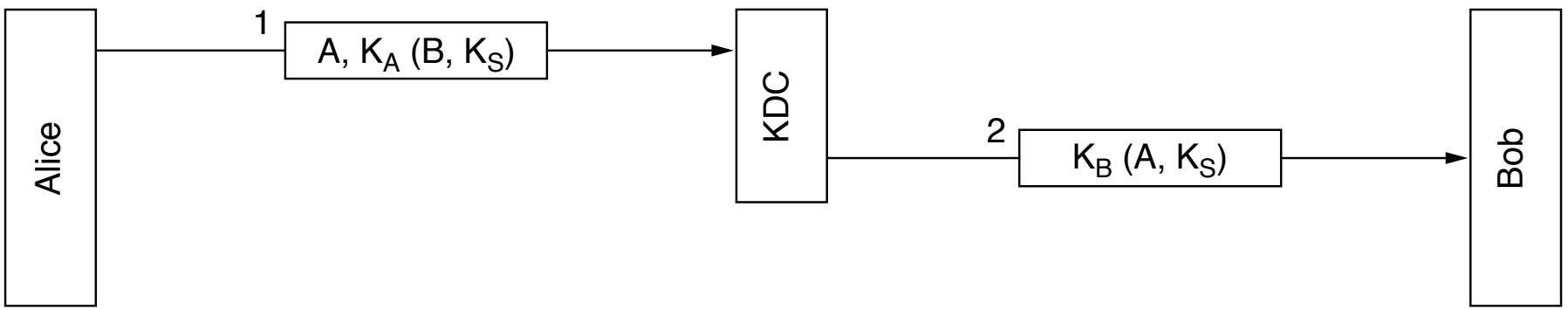
Authentification via un KDC

esil

☞ Dans cette approche, on suppose que le KDC (Key Distribution Center) est un organisme dans lequel tout le monde a confiance.

☞ Chaque utilisateur possède une clé secrète qu'il partage avec le KDC.

☞ Un premier protocole simple :



Est-il correct ?

Authentification via un KDC

esil

☞ Non ! Le protocole précédent à une faille. Il est possible qu'Eve réalise une attaque par rejeu à partir du message 2.

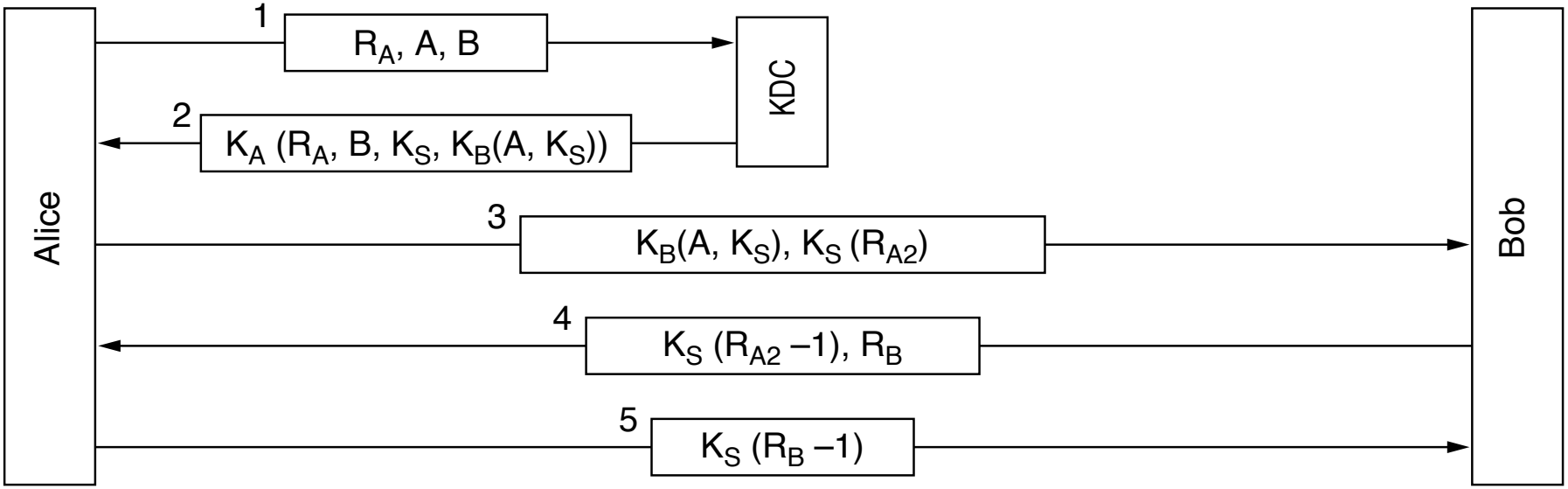
☞ Parade contre les attaques par rejeu :

- horodatage des messages. Mais les horloges ne sont jamais exactement synchronisées ce qui permet d'attaquer par rejeu durant un court laps de temps.
- utilisation d'un grand nombre aléatoire à utilisation unique (nonces) dans chaque message. Problème : les nonces doivent être mémorisés éternellement, panne de l'ordinateur.
- associer les nonces et l'horodatage. Bonne solution.
- utiliser un protocole question-réponse du type Needham-Schroeder

Authentification via un KDC

esil

☞ Protocole d'authentification de Needham-Schroeder

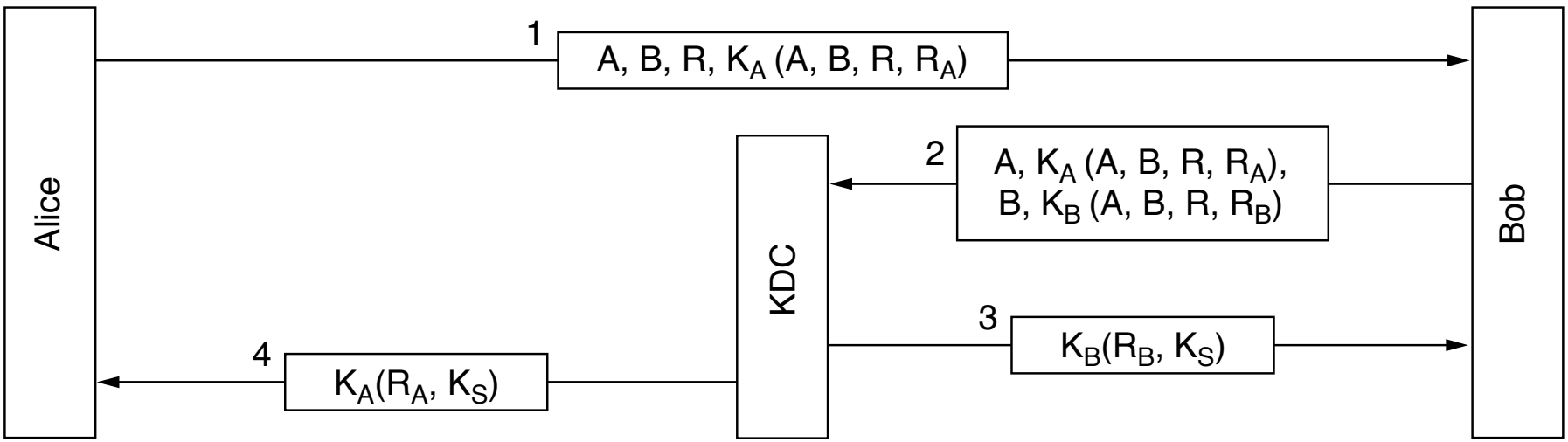


Y-a-t-il une faille ?

Authentification via un KDC

esil

☞ Protocole d'authentification de Otway et Rees



Authentification via Kerberos

esil

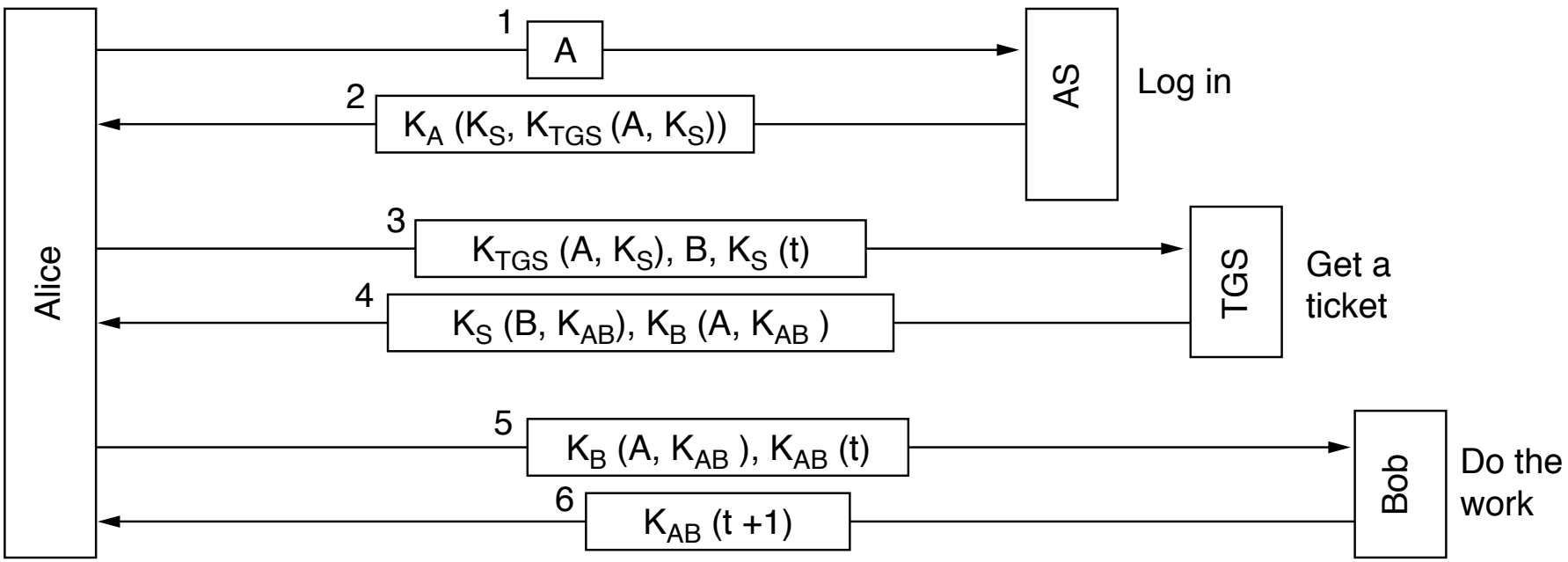
☞ Présentation de Kerberos :

- c'est un protocole d'authentification conçu pour permettre à un utilisateur d'accéder de manière sécurisée aux ressources du réseau
- élaboré par le MIT, il est utilisé dans beaucoup de systèmes réels (ex : windows 2000)
- il est basé sur une variante du protocole Needham-Schroeder
- il suppose que les horloges sont synchronisées
- il nécessite trois serveurs :
  1. un serveur d'authentification (Authentication Serveur) qui joue le rôle du KDC
  2. un serveur de vérification de ticket (Ticket-Granting Serveur) qui délivre des tickets permettant de prouver que le possesseur d'un ticket et bien celui qu'il prétend être.
  3. le serveur (Bob) qui va effectuer le travail demandé par Alice.

Authentification via Kerberos

esil

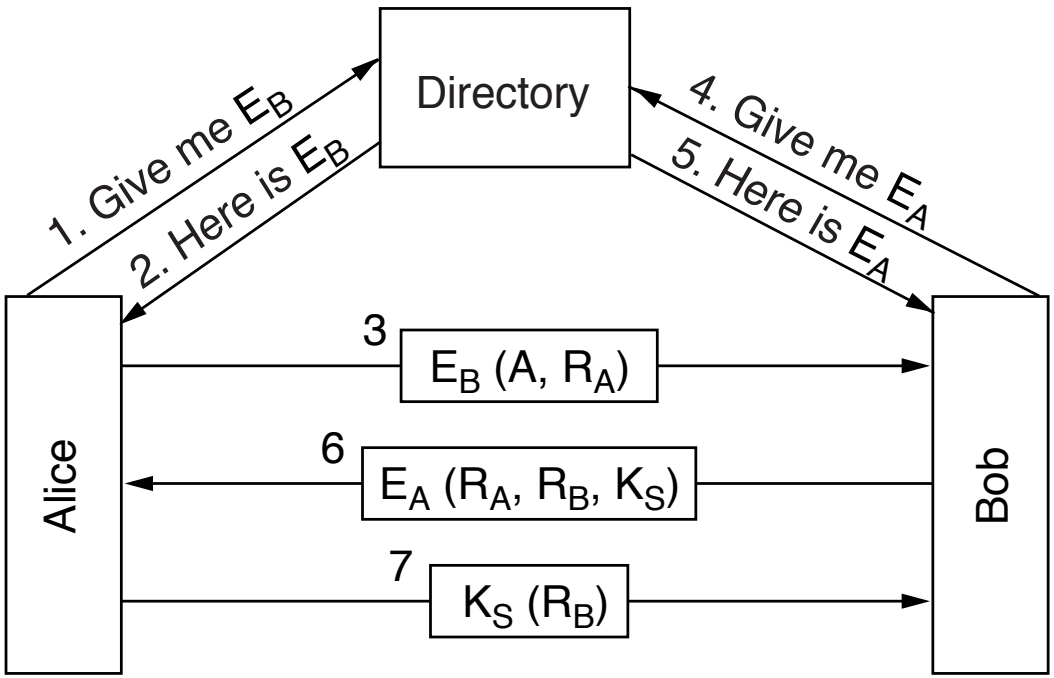
☞ Fonctionnement de Kerberos version 4 :



Authentification par cryptographie à clé publique

esil

☞ Authentification mutuelle en utilisant des clés publiques :



Que peut faire Eve ?

Plan

Pretty Good Privacy (PGP)

esil

☞ Présentation :

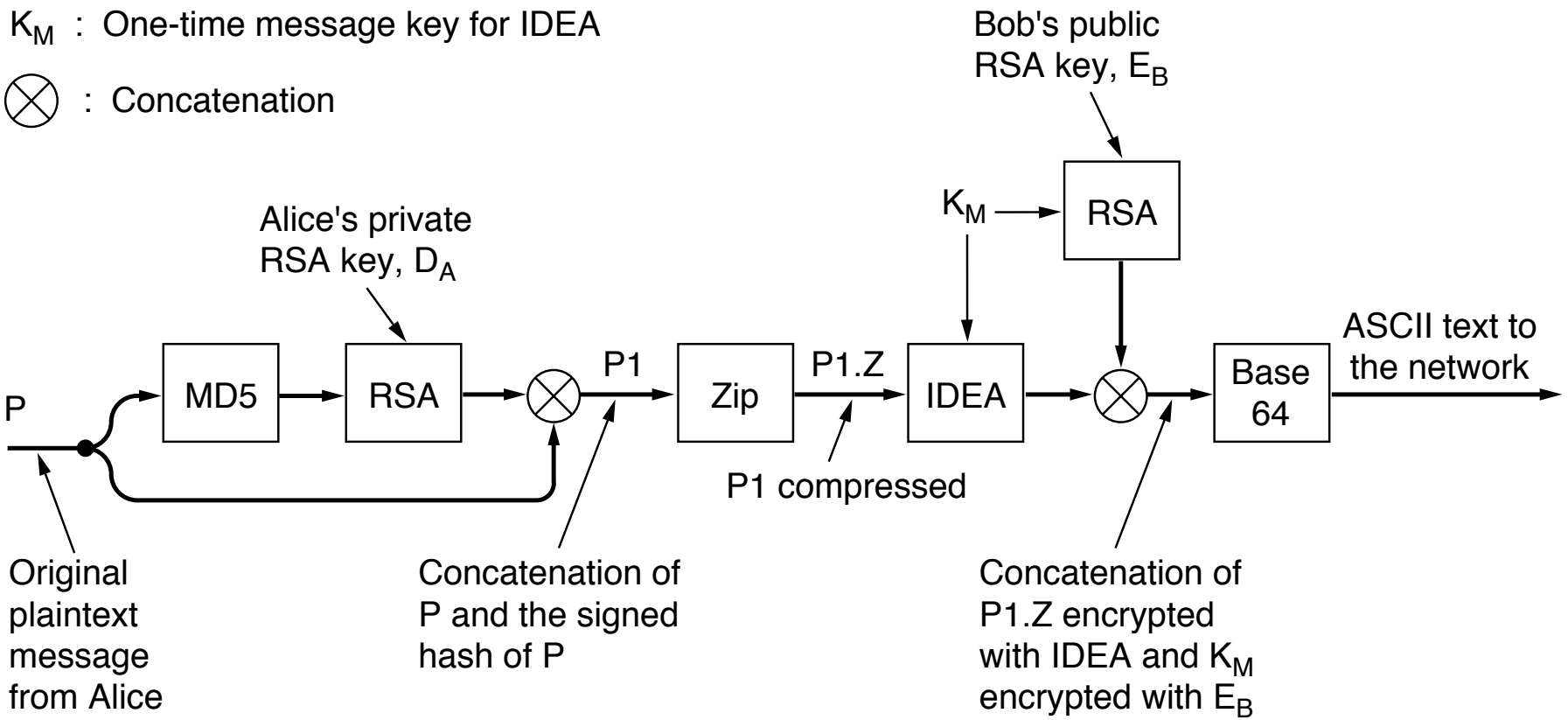
- conçu par P. Zimmermann : “si la vie privée est hors-la-loi, seuls les hors-la-loi auront droit à une vie privée”.
- c’est un package complet de sécurité du courrier électronique assurant
  - la confidentialité,
  - l’authentification,
  - les signatures nmériques,
  - la compression.
- PGP est distribué gratuitement (open source) et ses sources sont disponibles
- fonctionne sur de nombreuses plateformes (UNIX, Linux, Windows, Mac OS)
- plusieurs versions existent (Open PGP, Privacy Guard, ...)

☞ Outils utilisés :

- PGP chiffre les données à l’aide de IDEA
- la gestion des clés repose sur RSA
- le contrôle d’identité sur MD5
- la compression des données utilise ZIP

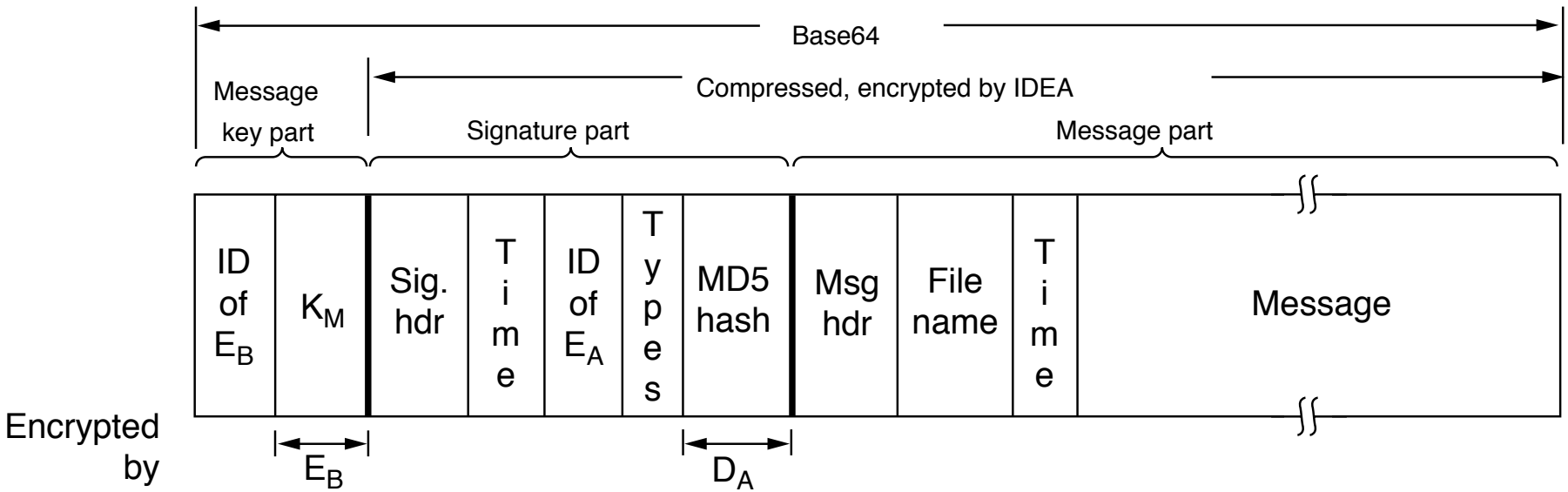
Fonctionnement de PGP

esil



Structure d'un message PGP

esil



Gestion des clés PGP

esil

☞ Chaque utilisateur conserve localement deux structures de données

- un anneau de couples <identifiant/clé privée>
- un anneau de couples <identifiant/clé publique>

☞ Les clés sont protégées sur le disque grâce à un chiffrement au moyen d'une phrase (la clé).

☞ Posséder plusieurs clés permet aux utilisateurs de changer de clés périodiquement, ou lorsqu'une clé risque d'être compromise. Le changement de clés est effectué grâce aux identifiants.

☞ Notion de degré de confiance d'une clé publique...

☞ Possibilité d'obtenir des clés publiques à l'aide de certificats X.509.

Privacy Enhanced Mail (PEM)

esil

☞ Présentation :

- standard officiel de l'internet (RFC 1421-1424)
- similaire à PGP : garantit le secret et l'authentification du courrier électronique
- gestion de clés par des certificats X.509 délivrés par des CAs chapeautés par un root
- N'a jamais été utilisé

☞ Fonctionnement :

1. message à envoyer
2. traitement initial des espaces
3. calcul du hachage MD5 du message
4. résultat du hachage concaténé avec le message
5. chiffrement avec DES (clé de 56 bits)
6. message chiffré codé en base 64
7. transmission du résultat.

Secure/MIME

esil

☞ Présentation :

- standard officiel de l'internet (RFC 2632-2643)
- garantit le secret, l'authentification du courrier électronique, la non-répudiation, le contrôle d'intégrité
- gestion de clés par des certificats X.509, mais c'est cette fois-ci à l'utilisateur de définir quelles sont ses ancres de confiance

Plan

Présentation

esil

Le Web est très souvent utilisé pour des transactions financières :

- achat de marchandises
- suivi de comptes bancaires
- bourse, ...

➥ les connexions web doivent être sécurisées
➥ package de sécurité présenté par Netscape Communications Corp. : SSL

☞ SSL construit une connexion sécurisée entre deux sockets assurant :

- la négociation des paramètres entre le client et le serveur
- l'authentification mutuelle
- la confidentialité des données
- l'intégrité des données

☞ SSL a été standardisé par l'IETF (RFC 2246) sous le nom de TLS (Transport Layer Security) en 1996.

SSL et la pile TCP/IP

esil

☞ Place de SSL dans la pile de protocoles :

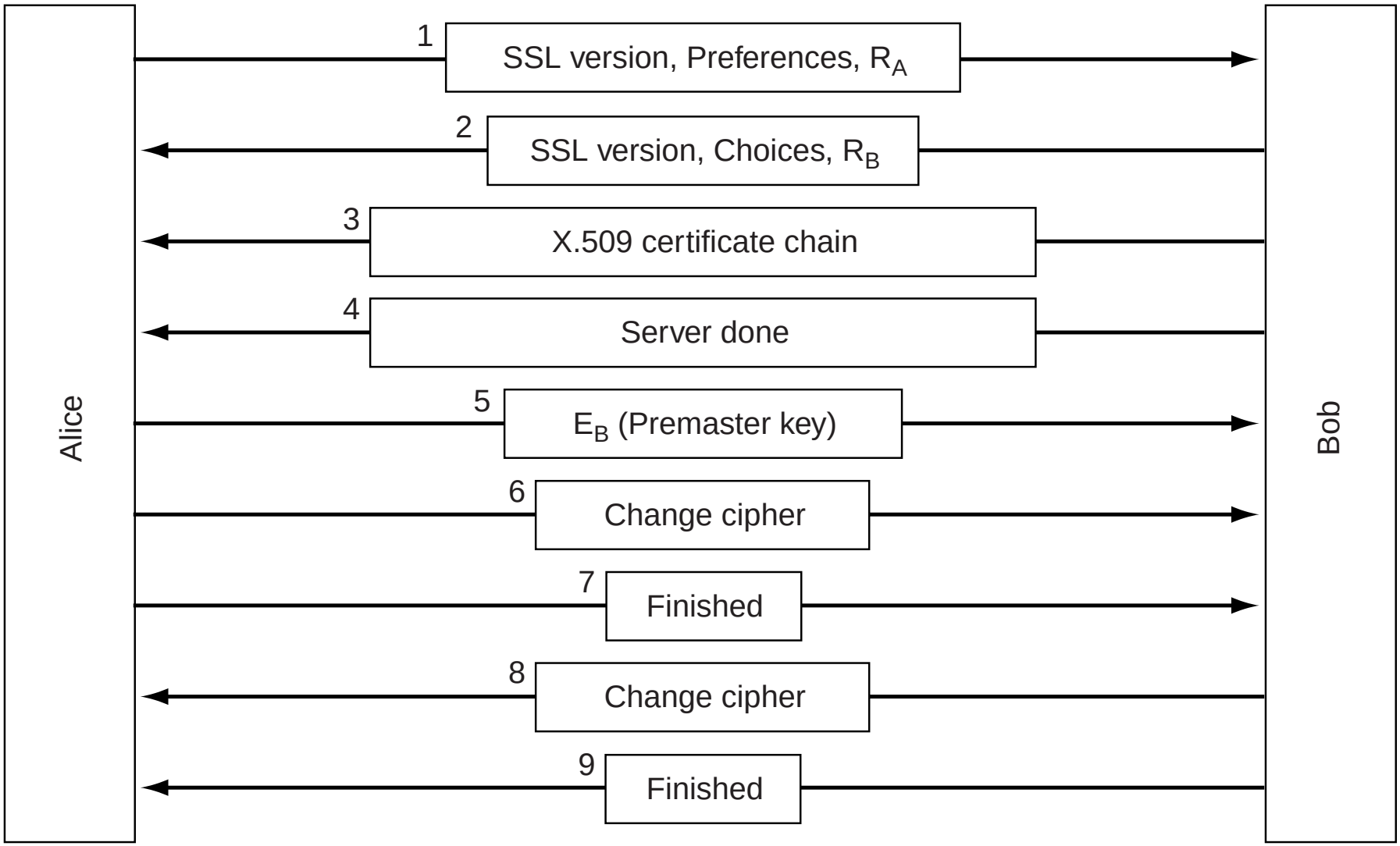
Application (HTTP)
Security (SSL)
Transport (TCP)
Network (IP)
Data link (PPP)
Physical (modem, ADSL, cable TV)

☞ SSL est constitué de deux sous-protocoles :

- un protocole d'établissement de la connexion sécurisée
- un protocole de transport

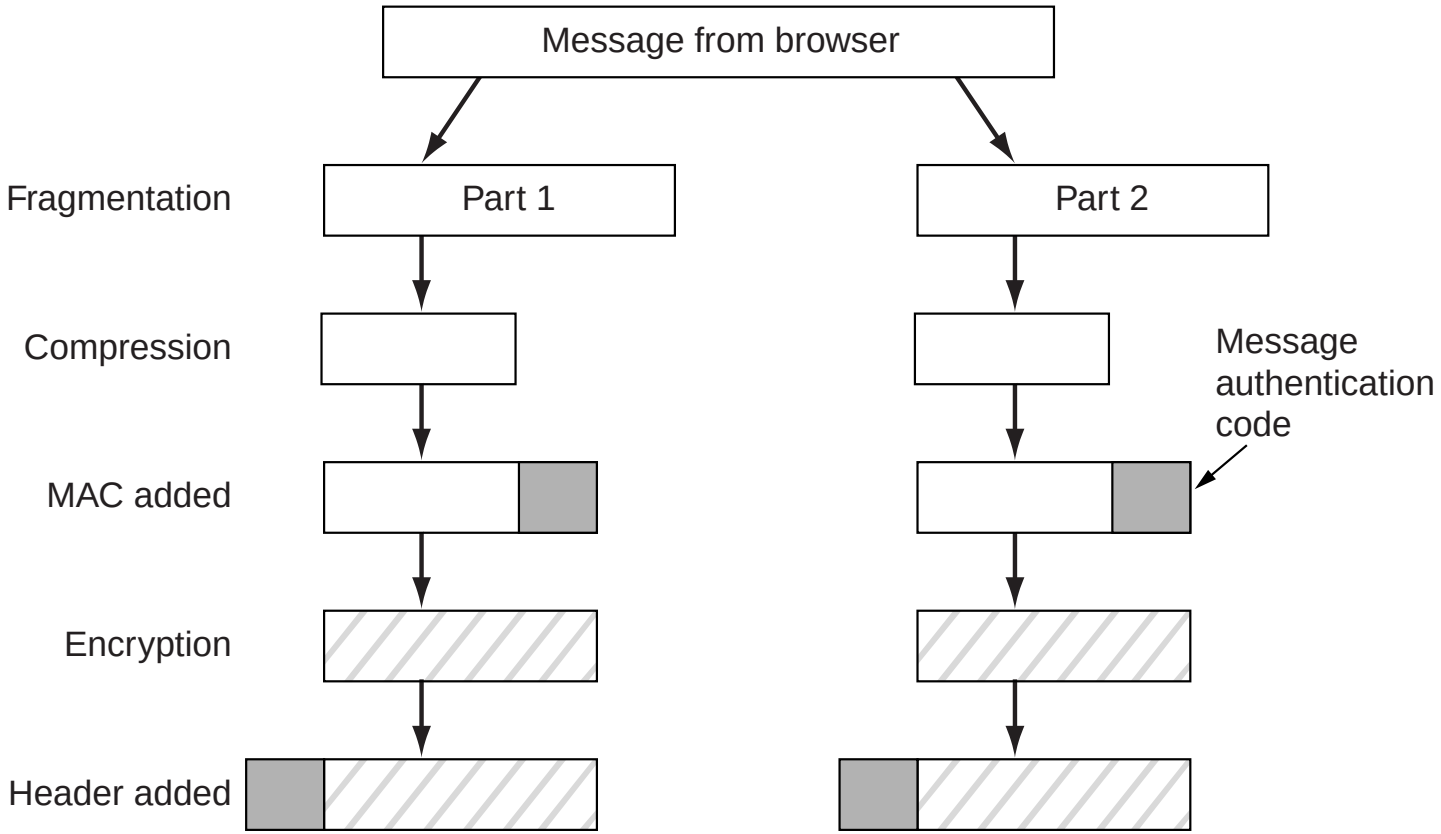
Etablissement de la connexion sécurisée

esil



Le transport des données

esil



- la fragmentation crée des blocs de 16Ko
- la clé secrète est concaténée avec le texte compressé
- le résultat est haché (souvent avec MD5, parfois SHA-1) puis utilisé comme MAC
- le tout est chiffré (souvent RC4 - clé de 128 bits, parfois triple DES)

Plan

Conclusion

esil

☞ Vie privée :

- la technologie permet à l'état de s'immiscer dans la vie privée des personnes
- la technologie permet à toute personne de protéger efficacement sa vie privée
- la sécurité d'un pays peut-elle justifier d'être privé de vie privée ?

=> mécanisme d'anonymat

☞ Liberté d'expression :

- confrontation du web mondial et des lois nationales
- problème de la censure

=> utilisation de services pour l'éternité (Freenet, PASIS, Publius) et de la stéganographie