Initiation à la cryptographie et Internet

Sommaire

- La sécurité des systèmes d'information
- Les méthodes de cryptage
  - Cryptographie symétrique
  - Cryptographie Asymétrique
- La signature numérique
- Les certificats numériques et les PKI
- Cryptographie et Internet
  - Le protocole SSL

Sécurité des SI : contexte

- Avènement des réseaux ouverts (Internet / Intranets / Extranets)
- Multiplication des ressources électroniques
- Développement du commerce électronique

Les 5 fonctionnalités d'un système sécurisé

- **Confidentialité** : L'information ne peut être déchiffrée
- **Authentification** : Identité valide
- **Contrôle d 'accès** : Accès sélectif à des ressources
- **Intégrité** : Les données ne sont pas altérées
- **Non-répudiation** : Un échange a bien lieu

Le cryptage

- Assure la confidentialité

- chiffre à substitution simple (J. César)
- Carré de Vigenère (1586)
- Machine à rotors Enigma (1938)
- Cryptographie asymétrique (Diffie -Hellman - 1976)
- Rivest-Shamir-Aldeman (RSA 1978)
- Ellis et Cocks (1969,1973)

Cryptographie symétrique

- L 'émetteur et le récepteur utilisent la même clé pour crypter et décrypter
- Avantages :
  - Rapidité de l 'algorithme
  - Simplicité de mise en œuvre
- Inconvénients :
  - l'expéditeur d'un message doit au préalable communiquer la clé au destinataire par un canal sûr
  - l'expéditeur ne peut employer une clé qu'avec un destinataire

Algorithmes et taille des clés

- Les algorithmes sont basés sur des fonctions de permutation complexes
- Taille d'une clé : nombre de bits servant à coder la clé :
  - Clé à 56 bits : nombre codé sur 56 bits donc compris entre 0 et 2^{56}
  - Pour "briser" la clé : méthode de la force brute. On doit tester toutes les solutions …
  - Passer de 56 à 128 bits = multiplier le temps de recherche par 2^{76}
- DES (Data Encryption Standard)

Cryptographie asymétrique

- Paire de clés (clé publique et clé privée)
- Avantages
  - Permettre les échanges ponctuels
  - limiter le nombre de clés
- Inconvénients
  - Pas d'authentification
  - Lenteur des algorithmes

Algorithme

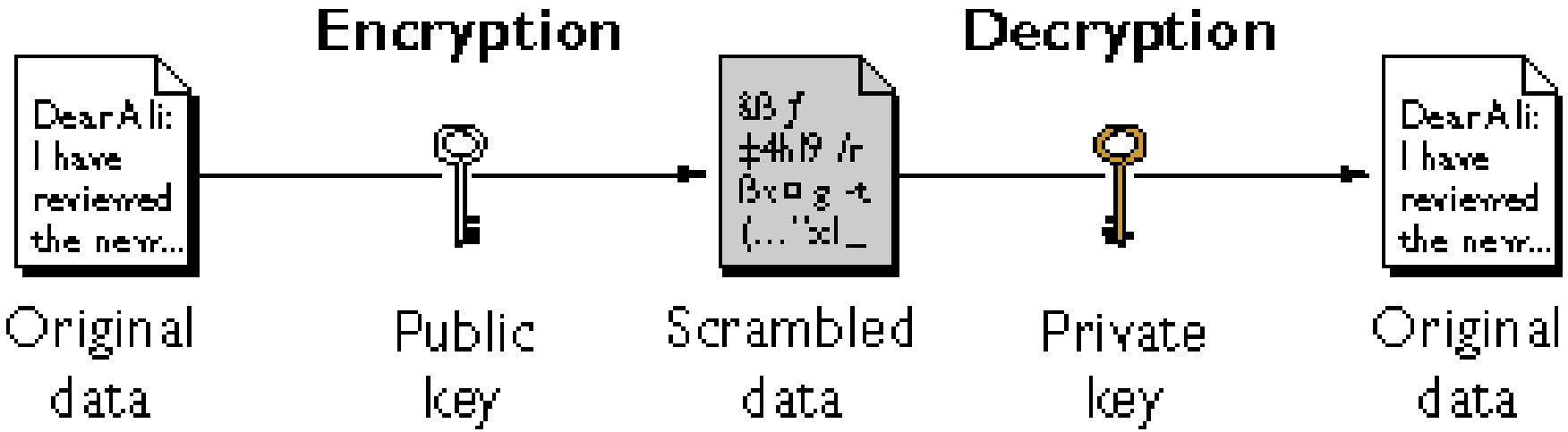
- Les algorithmes sont basés sur la théorie des nombres :

PxQ=N

et sur l'arithmétique "modulo"

$$P^x \pmod{Q} = M$$

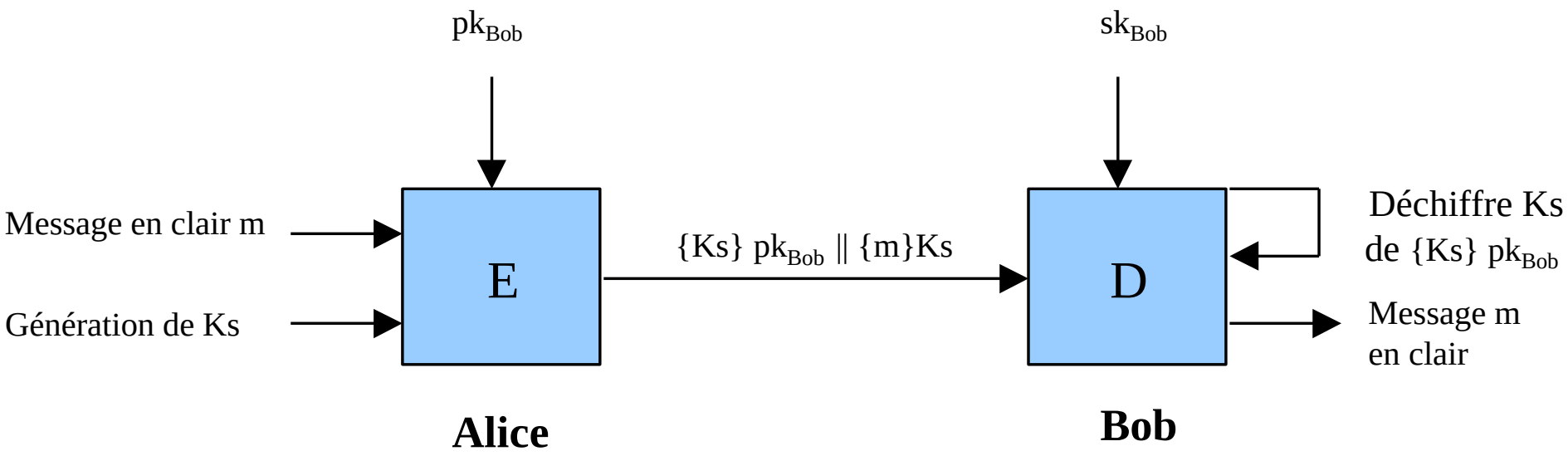
Cryptographie asymétrique



Cryptographie asymétrique

- 1. Supposons que Alice et Bob veuillent s'échanger des messages :
  - Alice et bob génèrent leur paire de clés (publique et privée)
  - Alice envoie sa clé publique à Bob
  - Bob utilise la clé publique d'Alice pour crypter un message pour Alice
  - Alice décrypte ce message en utilisant sa clé privée

Chiffrement Hybride (Enveloppe Numérique)



L'émetteur Alice utilise la clé publique pk_{Bob} pour chiffrer une clé de session Ks d'un algorithme symétrique : {Ks} pk_{Bob}
L'émetteur chiffre le message m avec la clé Ks : {m} Ks

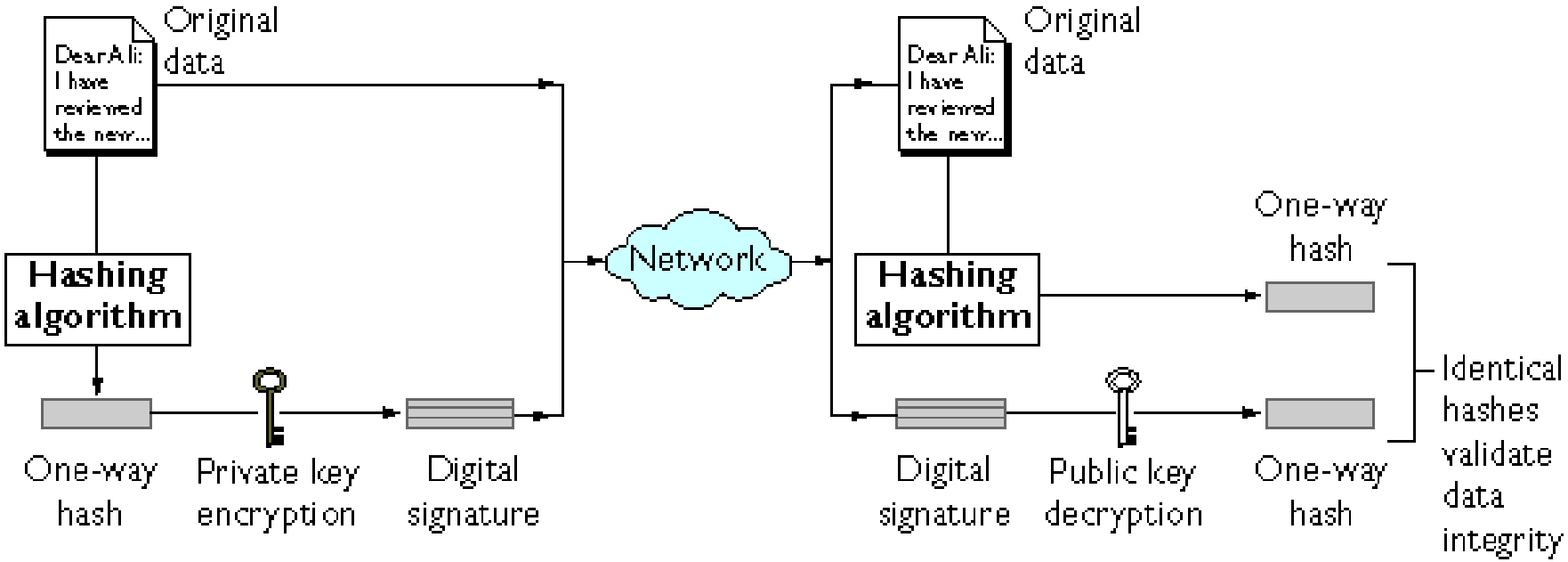
Le destinataire Bob utilise la clé privée sk_{Bob} pour déchiffrer la clé de session Ks
Le destinataire utilise la clé de session Ks déchiffrée pour déchiffrer le message m

Algorithmes

- DES : adopté comme standard en 1976 par la NSA. DES fonctionne en trois étapes :
  - permutation initiale et fixe d'un bloc.
  - le résultat est soumis à 16 itérations d'une transformation, ces itérations dépendent à chaque ronde d'une autre clé partielle de 48 bits. Cette clé de ronde intermédiaire est calculée à partir de la clé initiale de l'utilisateur (grâce à un réseau de tables de substitution et d'opérateurs XOR). Lors de chaque ronde, le bloc de 64 bits est découpé en deux blocs de 32 bits, et ces blocs sont échangés l'un avec l'autre. Le bloc de 32 bits ayant le poids le plus fort (celui qui s'étend du bit 32 au bit 63) subira une transformation.
  - le dernier résultat de la dernière ronde est transformé par la fonction inverse de la permutation initiale.
- 3DES, IDEA, AES
- Blowfish : utilisé dans de nombreux logiciels propriétaires et libres (dont GnuPG et OpenSSH).

La signature Numérique

- Permet de vérifier qu'un message n'a pas été altéré



Fonctionnement

- 1.L'expéditeur calcule l'empreinte de son message à l'aide d'une fonction de hachage.
- 2.L'expéditeur chiffre l'empreinte avec sa clé privée.
- 3.L'expéditeur chiffre l'empreinte chiffrée avec le texte clair à l'aide de la clé publique du destinataire.
- 4.L'expéditeur envoie le message chiffré au destinataire.
- 5.Le destinataire déchiffre le message avec sa clé privée.
- 6.Le destinataire déchiffre l'empreinte avec la clé publique de l'expéditeur.
- 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.

MD5

- L'algorithme de hachage MD5 est le plus courant (Message-Digest Algorithm)
- Le résultat est un nombre de 32 caractères hexadécimaux.
- Il existe plusieurs façon de contourner un hash MD5.
  - l'attaque par « brute-force ».
  - créer des collisions, c'est à dire la possibilité de générer plus ou moins facilement des chaînes différentes qui ont le même hash MD5. (2004)
- SHA1, SHA2 … actuellement SHA-128

Les Certificats Numériques

- C'est une preuve irréfutable de l'identité d'un émetteur. Un certificat contient généralement :
  - La clé publique de l'émetteur
  - Son identité
  - La signature numérique de l'autorité de certification (CA) de référence

- Une CA est une "tierce partie de confiance". Son rôle est de gérer les identités et les clés publiques d'une communauté d'utilisateurs.

- http://www.ssi.gouv.fr/fr/sigelec/index.html
- http://www.ssi.gouv.fr/fr/confiance/evalcertif.html

Les PKI

- Une autorité de certification chargé de la gestion des clés.
- Une autorité d'enregistrement (Registration Authority, RA) qui sert d'intermédiaire entre les utilisateurs et la CA. Son rôle est d'identifier (physiquement ou non) les utilisateurs et de valider les demandes de certificats auprès de la CA.
- Un système de gestion des certificats et des listes de révocation (ou plus largement, un outil de stockage et de gestion des clés et de l'identité des utilisateurs), qui peut par exemple être un annuaire (LDAP ou X500) ou bien encore un système de carte à puces
- Une politique de sécurité

Cryptographie et Internet

SSL

Communication sur Internet utilisant un certificat entre Alice et Bob (1/3)

- Alice crée une clé secrète ainsi qu'une clé publique.
- Elle envoie la clé publique à une autorité de certification, à qui elle demande un certificat numérique. Pour authentifier Alice, cet organisme vérifie les informations fournies par Alice.
- L'organisme de certification envoie un certificat numérique qui authentifie la clé publique d'Alice. Sur ce certificat se trouve la signature numérique du tiers de confiance qui peut être vérifiée par toute personne connaissant la clé publique de cet organisme.
- La clé publique de l'autorité de certification est fournie à ceux qui en ont besoin, dont Bob.

Communication sur Internet utilisant un certificat entre Alice et Bob (2/3)

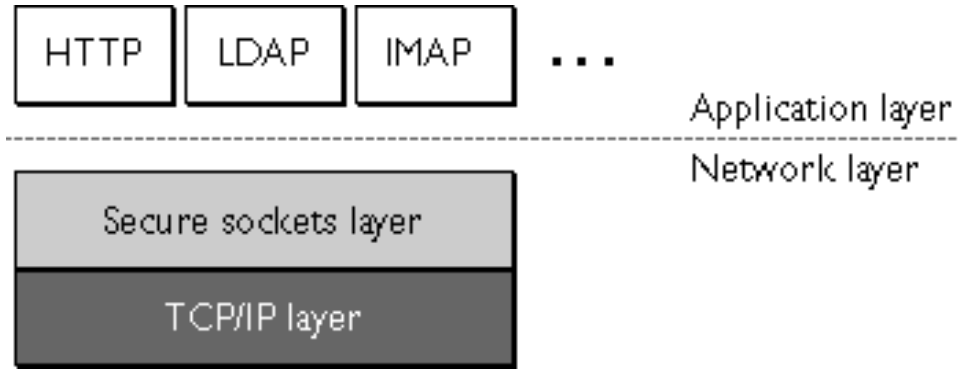
- Alice signe numériquement le message qu'elle envoie à Bob : Elle crée une empreinte du message en lui appliquant une fonction de hachage. L'empreinte est ensuite chiffrée à l'aide de la clé secrète d'Alice ce qui donne la signature numérique du message.
- Cette signature est envoyée à Bernard en même temps que le message. Alice envoie aussi son certificat numérique, qui contient sa clé publique.

Communication sur Internet utilisant un certificat entre Alice et Bob (3/3)

- Bob utilise la clé publique correspondant à l'autorité de certification pour vérifier la signature numérique officielle apposée sur le certificat. Il est alors certain que le certificat est authentique et que la clé publique qui l'accompagne appartient à Alice.
- Il utilise alors cette clé pour déchiffrer la signature numérique d'Alice et obtient donc le condensé du message. Enfin, Bob applique la fonction de hachage au message envoyé par Alice et obtient ainsi un condensé du message.
- Si ce condensé est identique à celui qui est obtenu par le déchiffrage de la signature numérique d'Alice, Bob est certain que le message provient bien d'Alice et qu'il n'a pas été altéré par une tierce personne

Le protocole SSL/TLS

- Tourne au dessus de TCP/IP
- Permet d'établir une connexion sécurisée entre un client SSL (le navigateur) et un serveur SSL



- Se décompose en deux sous-protocoles :
  - SSL handshake
  - SSL record

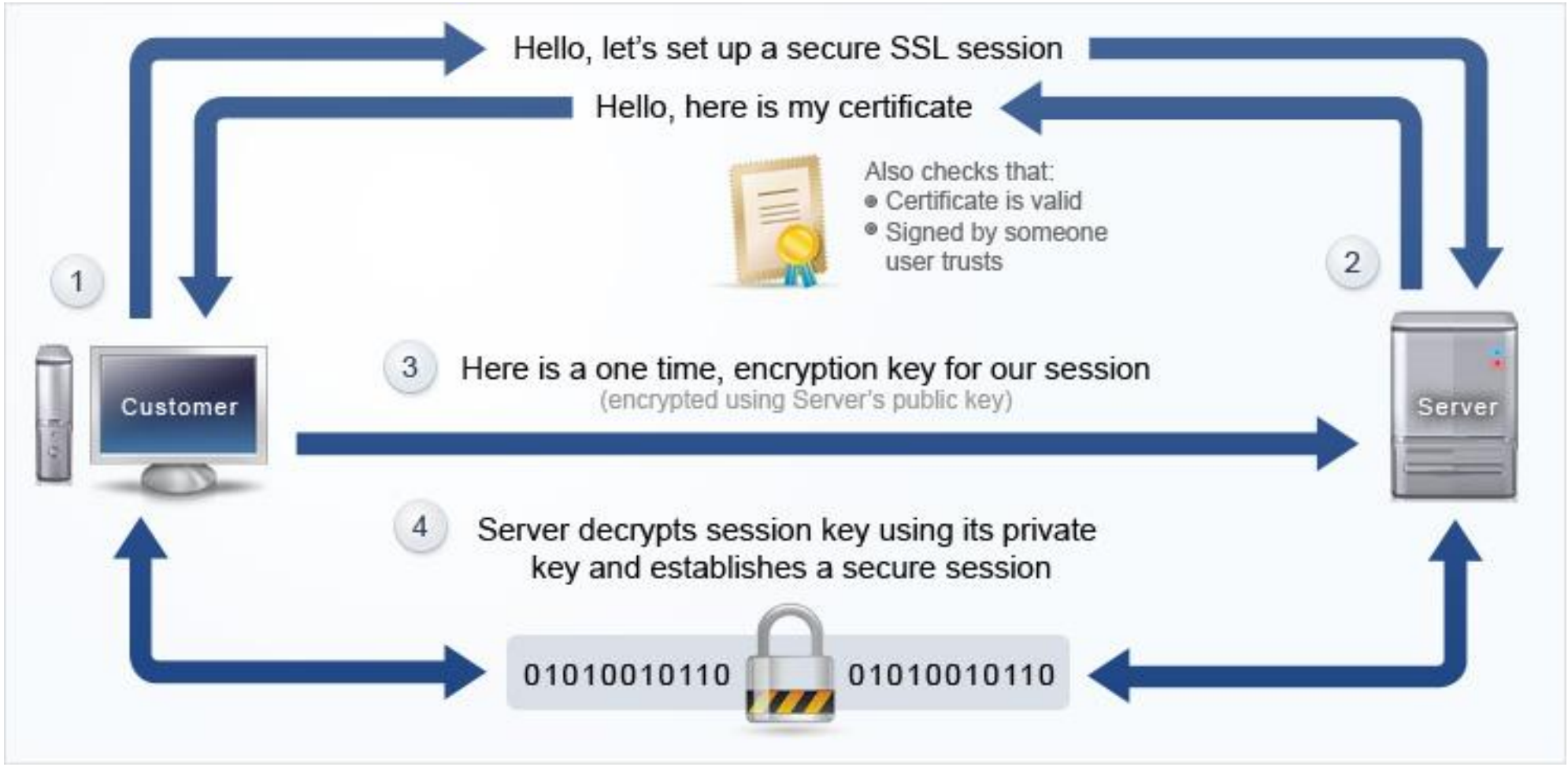
SSL Handshake

- Authentifie le serveur au client
- Permet au client et au serveur de choisir un algorithme ce cryptage commun
- Utilise la cryptographie à clé publique pour générer une clé de cryptage
- Établie une connexion cryptée SSL

SSL+Apache+PHP

- Installer Apache-SSL ou mod_ssl pour impléménter ssl dans Apache, bibliothèque OpenSSL, un toolkit pour mod_ssl.
- Générer une clé privée
- Créer une requête de certificat (CSR)
- Obtenir un certificat signé (Symantec-ex Verisign ou Thawte) qui permette d'attester de l'identité de l'émetteur de la clé

Fonctionnement d'une requête sécurisée



En php

- La fonction md5() est dépréciée et ne doit, en théorie, plus etre utilisée.
- En effet, une faille permettant de diminuer considérablement le nombre d'opérations par une attaque force brute a été trouvée.
- De plus, il a été montré qu'il était possible de créer volontairement des collisions : les hashs MD5 sont constitués de 32 caractères alphanumériques. Ainsi, le nombre de hashs possibles est limité contrairement à la quantité des textes possible.
- On utilise depuis php5.5 une nouvelle API de hashage intégrée qui inclut la fonction password_ash()