Introduction à la cybérsecurité

Chapitre 1 Généralité

M. Remane NIZAR

PhD student in Coding, Cryptology, Algebra and application of UCAD

Data science, IA and IOT engineer of UVS - ATOS

Information System Security engineer of ESP

remane.nizar@ucad.edu.sn

Licence 2 Réseaux télécommunications

Deuxieme semestre

ISI 2022 - 2023

24 mai 2023

Plan

Matériels et Outils du cours

- Wireshark
- Packet Tracer dernière Version
- Kali Linux
- Metasploitable 2
- Machines virtuelles pour la Sécurité
- Pfsense

Objectifs du cours

Objectif général du cours

- L'**objectif de ce cours** est de permettre aux **étudiants de maitriser la sécurité des systèmes et réseaux**.

Objectifs spécifiques

- **Comprendre** les **concepts** de **bases** de la **sécurité** ;
- **Acquérir** les **connaissances théoriques et techniques** indispensables dans le **domaine de la sécurité des réseaux et systèmes** ;
- **Concevoir, implémenter et prendre en charge** la **sécurité des réseaux** et **systèmes** ;
- **Développer un esprit critique et des compétences** en **matière de résolution des problèmes de sécurité**.

Qu'est ce que la cybersécurité

Introduction

- La cybersécurité est la pratique consistant à protéger :
  - les systèmes ;
  - les réseaux
  - les programmes
- contre les attaques numériques.
- Par abus de langage on l'appelle également sécurité informatique ou sécurité des systèmes d'information ;
- ils peuvent également avoir des significations légèrement différentes ;
  - La sécurité informatique : elle se réfère à la protection des données, des systèmes et des réseaux informatiques contre les menaces internes et externes ;
  - La sécurité de système d'information : elle se concentre sur la sécurité des données, des applications, des processus métier, des systèmes et des réseaux.

- La cybersécurité : elle se concentre sur la sécurité des systèmes informatiques et des réseaux connectés à Internet.
- cyberattaques visent généralement à accéder à de l'information sensible, à la modifier ou à la détruire, à extorquer de l'argent à d'autres utilisateurs à l'aide de rançongiciels, ou à interrompre les processus d'affaires.
- Mettre en œuvre des mesures de cybersécurité efficaces s'avère particulièrement difficile de nos jours, car il existe plus d'appareils que de personnes dans le monde et les agresseurs deviennent de plus en plus innovants.

En quoi consiste la cybersécurité ?

- Une approche de cybersécurité efficace dispose de plusieurs couches de protection réparties :
  - les ordinateurs,
  - les réseaux,
  - les programmes
  - les données que l'utilisateur souhaite protéger.
- Les personnes, les processus et la technologie au sein d'une entreprise doivent tous se compléter pour créer une défense efficace contre les cyberattaques.
- Un système de gestion unifiée des risques liés à la sécurité peut automatiser les intégrations à travers les produits de sécurité Cisco sélectionnés et accélère les principales fonctions d'opération de sécurité, c'est-à-dire la détection, l'analyse et la correction.

Personnes

- Les utilisateurs doivent comprendre et respecter les principes de base relatifs à la sécurité des données, notamment en choisissant des mots de passe forts, en se méfiant des pièces jointes des courriels et en sauvegardant leurs données.En savoir plus sur les principes de base de la cybérsécurité grâce à ces 10 meilleurs conseils relatifs à la cybersécurité.
  - Utilisez des mots de passe forts et uniques pour chaque compte et changez-les régulièrement.
  - Activez l'authentification à deux facteurs pour ajouter une couche de sécurité supplémentaire à vos comptes en ligne.
  - Évitez de cliquer sur des liens ou de télécharger des pièces jointes provenant de sources non fiables ou inconnues.
  - Soyez prudent lorsque vous partagez des informations personnelles en ligne, notamment sur les réseaux sociaux.
  - Utilisez un logiciel antivirus et maintenez-le à jour pour protéger votre ordinateur contre les logiciels malveillants.
  - Évitez les réseaux Wi-Fi publics non sécurisés, ou utilisez un VPN pour sécuriser votre connexion. Sauvegardez régulièrement vos données importantes sur un disque dur externe ou sur le cloud.

- Assurez-vous que votre système d'exploitation et vos applications sont à jour pour bénéficier des dernières mises à jour de sécurité.
- Soyez vigilant en matière de phishing et apprenez à identifier les tentatives d'hameçonnage.
- Éduquez-vous régulièrement sur les dernières menaces en ligne et les meilleures pratiques de sécurité.

Cryptographie Moderne

- Cryptologie n'est pas la **sécurité** mais il n'ya pas de **sécurité sans la cryptologie** ;
- **Cryptographie n'est pas** seulement une **technique moderne,** ni un **produit de l'ère informatique**.
- Trouvé un scribe gravé des **hiéroglyphes en Égypte 2000 ans avant JC,** transformés sur une **pierre tombale de Khumholep 2** pour rendre **intelligible la description de sa vie.**
- Même époque **Jules Cesar** dans la **guerre des Gaules** décrivait un procédé de **substitution** aujourd'hui bien connu pour chiffrer leurs conversation.
- **Cryptographie moderne : dès 1970 à nos jours**
- **Cryptographie moderne :** basé sur des **problèmes mathématiques difficiles** tels que la **factorisation des nombre premier,** le problème de la **courbe elliptique** pour lesquels aucune solution connu n'a été trouvée jusqu'à présent

Quelques lexiques

- **Cryptographie :** Est l'art de rendre intelligible de chiffrer, de coder un message à ceux qui ne sont pas habilité à en prendre connaissance ;
- **Cryptanalyse :** c'est l'art pour une personne non habilité de décrypter, de décoder un message ;
- **Cryptologie :** Est la science qui engendre la cryptographie et la cryptanalyse ;
- **Cryptogramme :** Est un message chiffré ou codé ;
- **Sténographie :** Est la science qui dissimule (cache) l'existence du message ;
- **Clé :** Elle correspond à un nombre, un mot, une phrase, etc, qui permet grâce à l'algorithme de chiffrement, de chiffrer, de déchiffrer un message.

- **Chiffrer :** Transformer des informations claire en information intelligible à l'aide d'une convention secrète appelé clé, pour des tiers n'ayant pas connaissance du secret ;
- **Déchiffrer :** Retrouver l'information intelligible à partir de l'information chiffré en utilisant la convention secrète de chiffrement ;
- **Chiffre :** C'est le code, procédé, l'algorithme qui permet de crypter un message ;
- **Décrypter :** C'est retrouver l'information intelligible à partir de l'information chiffrée sans utiliser la convention secrète de chiffrement par contre, crypter ou encrypter n'a pas de sens clairement défini mais sont parfois utilisées à tort comme synonyme de chiffrer ;

Remarque

- Les termes **"cryptage" et "crypter"** sont des anglicismes dérivés de **l'anglais to encrypt,** souvent employés incorrectement à la place de **chiffrement et chiffrer.**
- En toute **rigueur, ces termes n'existent pas dans la langue française.**
- Si le **cryptage existait,** il pourrait être défini comme l'**inverse du décryptage,** i.e comme l'action consistant à obtenir un **texte chiffré** à partir d'un texte en clair sans connaître la clé.

Services de la cryptographie

Qualité d'un crypto système

Qualités demandées à un **système cryptographique** sont résumées par les mots clés suivants :

- **Intégrité des données :** Le message ne peut pas être falsifié sans qu'on s'en aperçoive
- **Confidentialité :** L'émetteur est sur que seul le destinataire pourra prendre connaissance du message car il est le seul à disposer de la clé de déchiffrement
- **Authentification :** le receveur est sur de l'identité de l'émetteur grâce à une signature
- **Non répudiation :** se décompose en trois

⋆ **Non répudiation d'origine :** l'émetteur ne peut nier avoir écrit le message
⋆ **Non répudiation de transmission :** l'émetteur du message ne peut nier avoir envoyé le message.
⋆ **Non répudiation de récepteur :** le receveur ne peut nier avoir reçu le message

Cryptographie symétrique

- Principe des **algorithmes de chiffrement à clé secrète (ou symétriques ou encore dits conventionnels)** sont ceux pour lesquels **l'émetteur et le destinataire partagent une même clé secrète**, autrement dit, la **clé de chiffrement et de déchiffrement est identique.**
- Emploi d'un algorithme à clé secrète lors d'une communication nécessite donc **l'échange préalable d'un secret entre les deux protagonistes à travers un canal sécurisé ou un autres techniques cryptographiques.**
- La figure suivante montre le **principe de chiffrement à clé secrète**

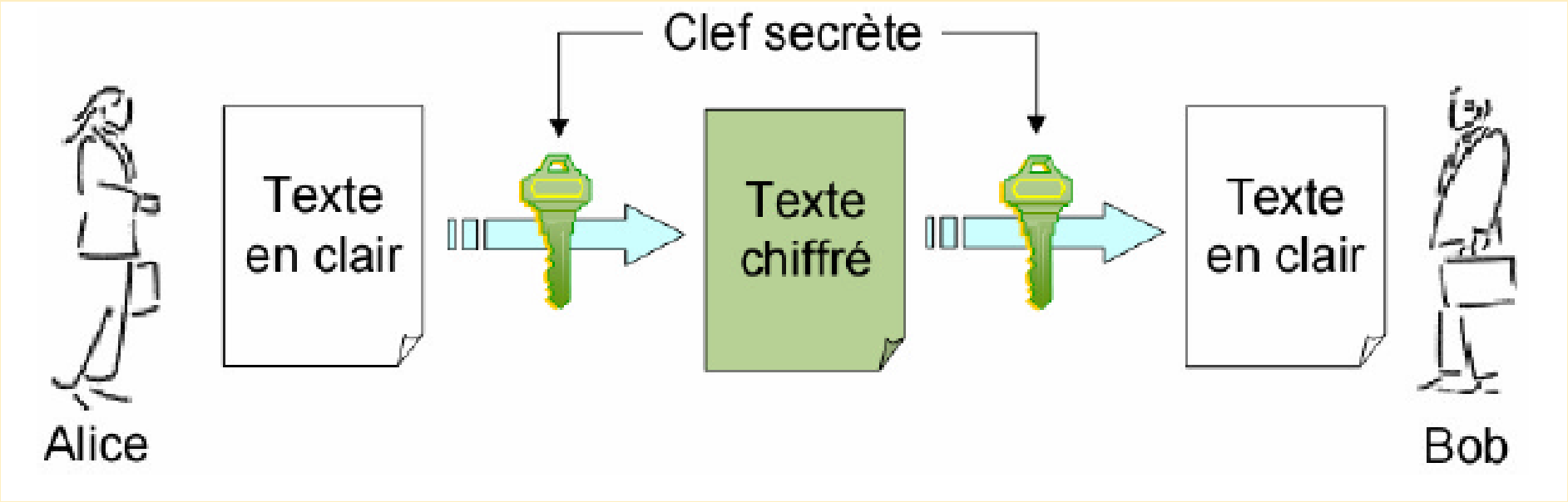


Figure – Schema cryptographie symétrique

Système de chiffrement, la **clé secrète doit être partagée entre les entités en communication d'où la nécessité d'avoir un canal sûr.**
Les algorithmes de **chiffrement symétrique sont décomposés en :**

Chiffrement par flux ou en continu(Stream cipher)

- **bit à Bit** sans attendre la réception entière des données.
- **Algorithmes les plus connu sont :**
  RC4, A5, ORYX, SEAL, E0 ; Py ;

Chiffrement par bloc (Bloc cipher en anglais)

- Consiste à **diviser les données en blocs de taille fixe**, chaque bloc ensuite sera **chiffré.**
  Algorithmes les plus connus sont :
  IDEA, BLOWFISH, FEAL, CAST, RC5, RC6, DES, 3DES et AES.

Longueur de la clé

- **Longueur de la clé de RC4 :**
  - Varie de **1 à 256 octets (8 à 2048 bits)** ;
  - En pratique, elle est souvent choisie de taille égale à **5 octets (pour 40 bits) ou 13 octets (pour 104 bits).**
- **Longueur de la clé DES**
  - **DES** est un système de chiffrement symétrique par **blocs de 64 bits**, dont **8 bits (un octet)** ;
  - **Longueur de la clé est de 56 bits**, ce qui signifie que seuls **56 bits servent réellement dans l'algorithme**.
- **Longueur de la clé AES**
  - **AES** est un système de chiffrement symétrique par **blocs de 128 bits**, dont **8 bits (un octet)** ;
  - La **clé fait 128, 192 ou 256 bits** ;
  - Les **16 octets en entrée** sont permutés selon une table définie au préalable.

Modes de chiffrement

Objectifs des modes opératoires

- Ne **concernent que le chiffrement par bloc.**
- Masquer les blocs clairs identiques.
- Deux **messages identiques chiffrés** avec la **même clé ne donnent pas les mêmes chiffrés.**

Mode ECB (Electronic Code Book)

- Consiste à chiffrer chaque bloc de texte en claire en un bloc de texte chiffré.

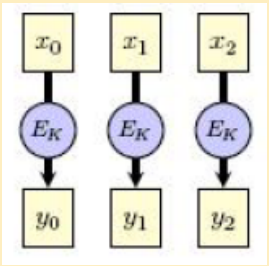


Figure – Mode ECB

- Pour effectuer un texte en mode ECB on effectue les opérations suivantes :
- **Chiffrement :** chaque bloc clair m_i est chiffré indépendamment et donne un bloc chiffre $C[n] = e(M[n])$ pour $n \geq 1$:
- **Déchiffrement :** chaque chiffré est déchiffré indépendamment pour donner le clair correspondant $M[n] = d(C[n])$ pour $n \geq 1$:
- **Idée la plus évidente :** "electronic codebook mode" (ECB) : découper le message en blocs de longueur N, chiffrer chacun indépendamment.
- **Conséquence :** deux blocs clairs identiques donnent toujours le même bloc chiffré pour une clé k fixé.
- **Avantages :** simple, parallélisable, possibilité d'accès aléatoire aux données déchiffrées, pas de propagation des erreurs.
- **Inconvénients :** les motifs répétés du clair sont apparents ; pas de **garantie d'intégrité :** un attaquant pourrait facilement modifier l'ordre des blocs, ou en répéter.

Exemple

Utilisons la permutation simple σ dans l'algorithme de chiffrement définie sur des bloc de 4 bits par :

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ Ce qui veut dire que :

- **Premier bit** de chaque bloc de texte en claire va être remplacer par **le deuxième**
- **Deuxième** bit de chaque bloc de texte en claire va être remplacer par le **troisième**
- **Troisième** bit de chaque bloc de texte en claire va être remplacer par le **quatrième**
- **Quatrième** bit de chaque bloc de texte en claire va être remplacer par le **premier**

Considerons le message claire **M= 101100010100101**

- Calculer C le chiffré du message M
- Calculer M le déchiffré de C

Mode CBC (Cipher Bloc Chaining)

- Un des modes les plus populaires
- Offre une solution à la plus part des problèmes du mode **ECB**
- Mode utilise la méthode de rétroaction comme le résultat du chiffrement, l'opérateur binaire XOR est appliqué entre le bloc actuel de texte en claire et le bloc précédent de texte chiffré et on applique ensuite l'algorithme de chiffrement au résultat de cette opération.
- Pour le tout premier bloc un bloc ayant un contenu aléatoire, appeler vecteur d'initialisation(IV). est une **valeur qui n'est pas secrète** dont le rôle est d'éviter que le chiffrement de deux clairs identiques soit identique.

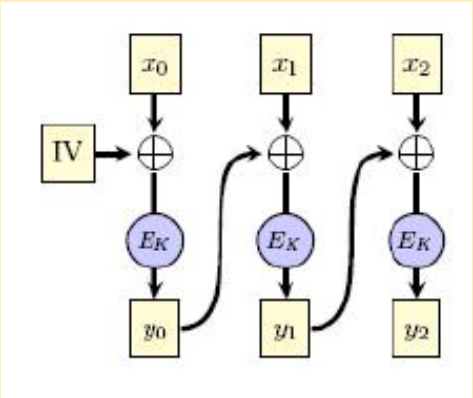


Figure – Mode CBC

- **Chiffrement :** On effectue par conséquent les opérations suivantes :
  $C[1] = e(M[1] \bigoplus VI)$
  $C[n] = e(M[n] \bigoplus C[n-1]) n \geq 1$
- **Déchiffrement :** On effectue les opérations suivantes
  $M[1] = e(C[1] \bigoplus VI)$
  $M[n] = e(C[n] \bigoplus M[n-1]) n \geq 1$
- **CBC est le mode le plus utilisé** (mais de moins en moins).
- **Pas de garantie d'intégrité,** mais un attaquant peut plus difficilement en tirer avantage.
- Le chiffrement ne peut se faire que **séquentiellement,** mais le déchiffrement peut se faire par **accès aléatoire.**

Exemple

Utilisons à nouveau la permutation simple σ définie par ;
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ comme algorithme de chiffrement pour chiffrer le même message $M = 1011100010100101$ qui produit les 4 blocs suivants :
$M[1] = 1011$; $M[2] = 0001$; $M[3] = 0100$ et $M[4] = 1010$
Choisissons le le vecteur d'initialisation(VI) : $VI = 1010$
et chiffrons en utilisant le mode CBC.

Chiffrements de Feistel.

- **Chiffrement de Feistel** est un chiffrement **itératif** par blocs opérant sur des **blocs de 2n bits.**
- **Fonction itérée f** est définie par :

$$f : F_2^n \times F_2^n \longrightarrow F_2^n \times F_2^n$$
$$(L_{i-1}, R_{i-1}) \longmapsto (L_i, R_i)$$

avec $L_i = R_{i-1}$ et $R_i = L_{i-1} \bigoplus f(R_{i-1}, K_i)$

- Quelle que soit la **fonction f** utilisée, un chiffrement de **Feistel est inversible.**
- Pour déchiffrer, il suffit d'utiliser le même processus à r tours en inversant l'ordre des clefs K_i (la fonction f est involutive par construction).

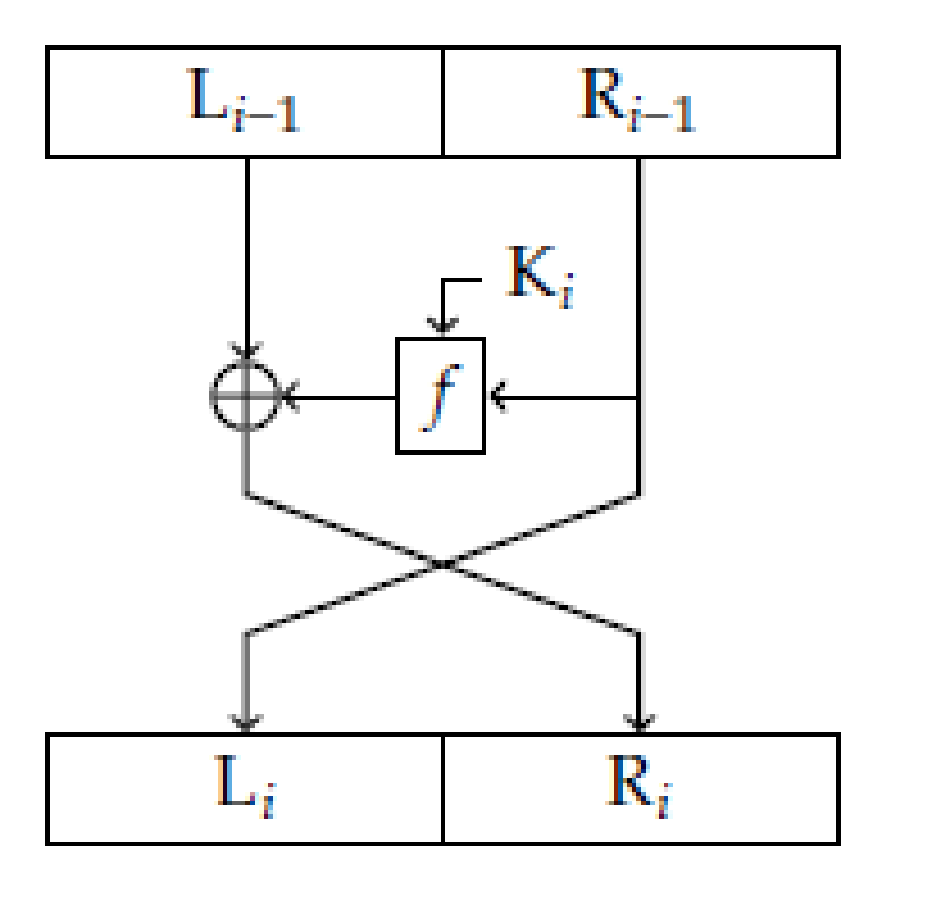
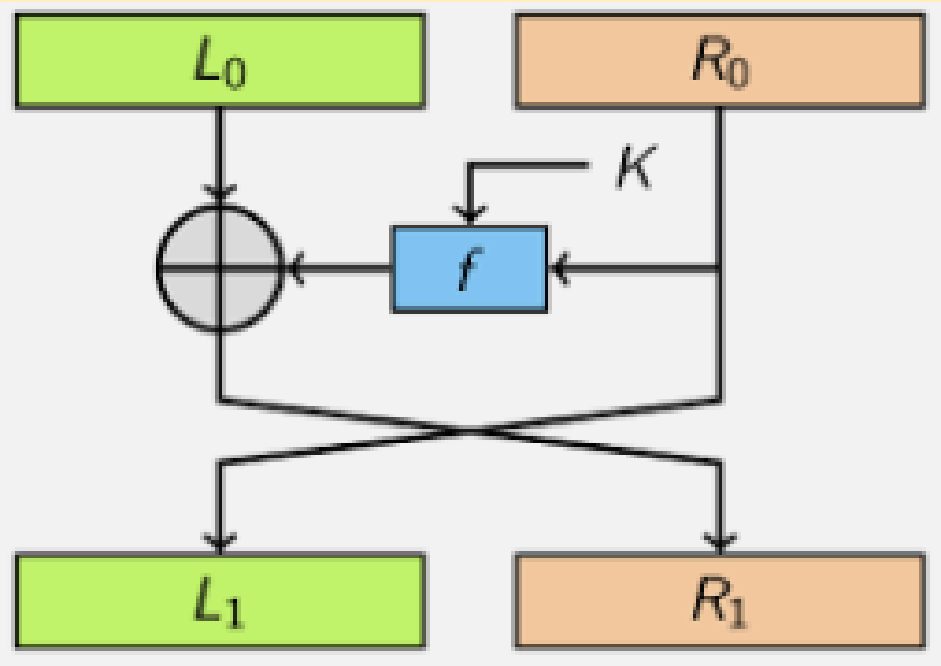


Figure – Feistel

$$L_i = R_{i-1} \text{ et } R_i = L_{i-1} \bigoplus f(R_{i-1}, K_i)$$

Exemple

Le réseau de Feistel de la figure suivante travaille sur un état de 8 bits



La fonction f prend en entrée une clé de 4 bits K et une donnée de 4 bits R_0, additionne bit- à-bit les deux entrées :

$f : \{0,1\}^4 \times \{0,1\}^4 \longrightarrow \{0,1\}^4$

. $(K, R_0) \longrightarrow f(K, R_0) = W = (w_1, w_2, w_2, w_2)$

$w_1 = u_1 \bigoplus u_2 \bigoplus u_3 \bigoplus 1$
$w_2 = u_3 \bigoplus u_1$
$w_3 = v_4 \bigoplus v_3 \bigoplus v_1 \bigoplus 0$
$w_4 = v_3 \bigoplus v_2$
avec $V = K = (v_1, v_2, v_3, v_4) = (k_1, k_2, k_3, k_4)$ et $U = u_1, u_2, u_3, u_4$.
On a $\mathbf{M = 10101011}$, $\mathbf{K = V} = R_0 = \mathbf{1011}$ **et** $L_0 = \mathbf{1010}$

1. Calculer le chiffrement C de M
2. Déchiffrer C

Data Encryption Standard (DES)

Historique

- C'est un **système cryptographique basé sur un schéma de Feistel.**
- Il est créé dans les **années 70 par le NIST (National Institute of Standard and Technology) (public en 1981)**
- l'**algorithme DES** a été l'algorithme de **cryptographie le plus usité jusqu'à l'an 2000.**
- Il a été récertifié depuis **(environ tous les 5 ans)** et est encore aujourd'hui utilisé (mais pas sous sa forme simple).
- Sa plus **récente version date de 1994.**
- Résultat d'un travail par **IBM,** avec des conseils de la **NSA (agence des services secrets américains).**
- L'algorithme est conçu pour **chiffrer et déchiffrer des blocs de données** constitués de **64 bits sous contrôle d'une clé 1 de 64 bits.**

Algorithme du DES

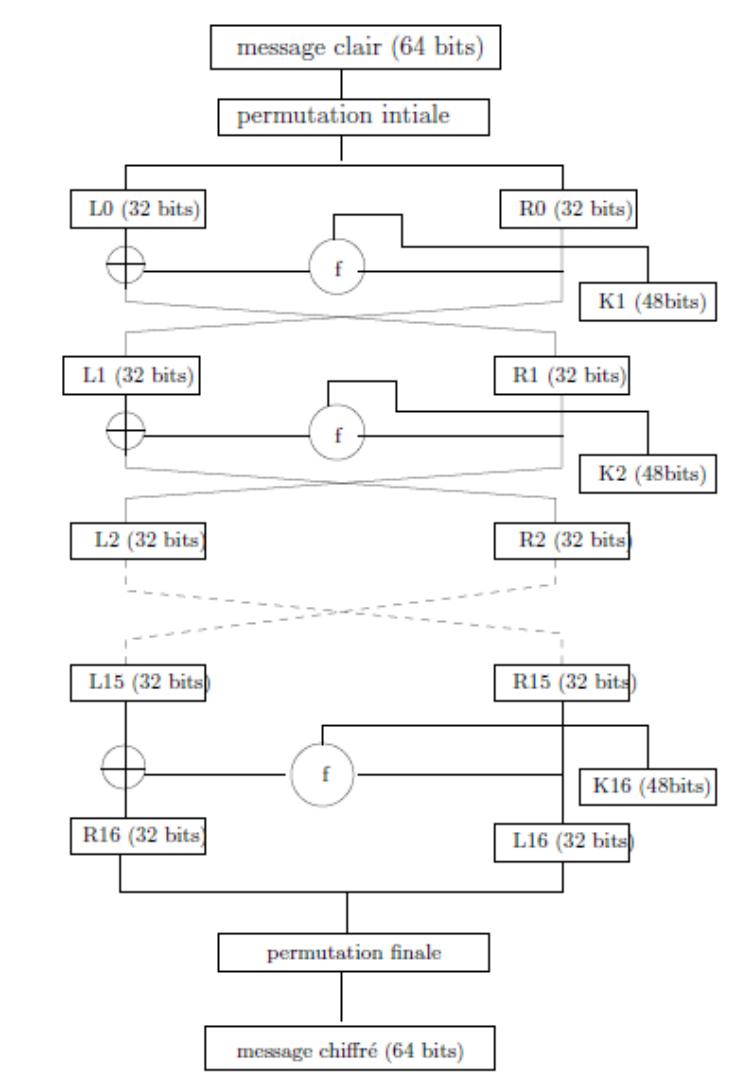


Figure – Architecture du DES

Algorithme

- Input : a message M and 16 subkeys $K_0, K_1, ...K_{15}$
- Z = IP(M)
- Split$(L_0, R_0) \longleftarrow Z$
- For i = 0 to 14, do
  - $L_{i-1} = R_i$
  - $R_{i-1} = L_i \oplus f(R_i, K_i)$

  End
- (Last round)
  - $R_{16} = R_{15}$
  - $R_{16} = R_{15} \oplus f(R_{15}, K_{15})$
- Z$\longleftarrow L_{16}||R_{16}$
- $Z = IP^{-1}(M)$

Advanced Encryption Standard AES

Historique

- L'**Advanced Encryption Standard a fait l'objet d'un appel d'offre datant de 1997.**
- Il s'agissait de **remplacer le DES** dont la **taille des clés (56 bits)** était devenue **trop petite pour les performances des ordinateurs modernes.**
- Les spécifications étaient une **longueur de blocs de 128 bits (ou de 256 bits)** et une **longueur de clé paramétrable : 128 ou 192 ou 256 bits**(des variantes sous le nom de Rijndael autorisent 160 ou 224 bits de clé) ;
- Parmi les **15 candidats sélectionnés Cinq aller en final (Rijndael, Serpent, Twofish, RC6 et MARS).**

- les **candidats retenus (en 2000)** sont des **belge nommé RIJNDAEL(Joan Daemen et Vincent Rijmen) (mais on l'appelle simplement l'AES)**.
- Standard **publié en 2001**
- C'est un chiffrement itératif, mais contrairement à 9 autres candidats, ce n'est pas un chiffrement de Feistel.

Principe

- L'**AES opère sur des blocs rectangulaires de 4 lignes et Nc colonnes,** dont chaque terme $x_{i,j}$(appelé octet ou byte) est composé de 8 bits

$$b = b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0$$

et peut être représentés **algébriquement sous forme de ploynômes de degrés $\leq$ 7**

$$b = b_7 X^7 + b_6 X^6 + b_5 X^5 + b_4 X^4 + b_3 X^3 + b_2 X^2 + b_1 X + b_0$$

à **coefficients dans $\mathbb{F}_2$**
La **clé peut être d'une longueur de 128, 156, ou 256 bits,** de même pour le message clair et le message chiffré.

Fonction de hachage

- Une **fonction de hachage** est une **application**(fonction publique) $H : \{0,1\}^* \longrightarrow \{0,1\}^n$ telle que :
  - **H** transforme un **message (binaire)** de **longueur quelconque** en un **message de longueur fixe (Fonction de Compression)** ;
  - pour tout x, H(x) est facile à calculer ; **(Facilement calculable)**
- Les images $H(x)$ **sont appelées hache ou empreinte(message digest ou hash en anglais).**
- La **probabilité** d'avoir deux messages avec le **même haché** doit être extrêmement faible.
- Le haché **ne contient pas assez d'informations** en lui-même pour permettre la reconstitution du texte original.

- On les utilise en cryptographie pour :
  - fournir un **condensé** de taille fixe ;
  - représenter précisément les données : la **détection des changements** dans le message est simplifiée.
- Dans la majorité des cas, elles seront utilisées pour créer une **signature numérique.**
- Qualité principale de ces **fonctions est que les algorithmes sont publics**.
- On parle de **"haché", de "résumé" , ou de "condensé"** pour nommer la caractéristique d'un texte ou de données uniques.

Algorithmes de fonction de hachage

Les fonctions de hachages comptent deux familles

- Celles n'utilisant pas de clés
  - **MD (Message Digest) :**
    - MD4, Rivest, 1990 ;
    - MD5, Rivest, 1992, empreinte sur 128 bits, RFC 1321
  - **SHA (Secure Hash Algorithm)** :
    - SHA1 inventé en 1995 produit des empruntes de 160 bits
    - SHA2 inventé plus tard en 2001 , fournit des empruntes entre 256 et 512 bits
- Tous ces fonctions des hachages sont basés sur le même mécanisme appelé la construction de Merkele-Damgard.
- **SHA3** inventé en 2015 par des chercheurs belges, produit un hache entre 256 à 512
- basé sur un mecanisme de KECCAK/construction de l'eponge completement different de Markele - Damgard

- **Celles utilisant des clés :**
  - Associé à une clé privé, elle permet le calcul d'un **sceau ou MAC**(Message Authentification Code) pour assurer :
  - Intégrité des données
  - Authentification de la source
  - Associé à un chiffrement asymétrique, elle permet le calcul de signatures, pour assurer :
  - Intégrité des données
  - Authentification de la source
  - Non-répudiation de la source

Scellement (MAC)

- Mécanisme qui consiste à calculer (ou sceller) une empreinte à partir d'un message et d'une clé privée pour :
  - Authentifier l'origine des données
  - Vérifier l'intégrité des données
- La scellement d'une empreinte génère :
  - un sceau ou
  - code d'authentification de message (MAC)
- Il est réalisé au moyen d'une fonction de hachage appliquée au message+clé privée :
  - Keyed-MAC (Keyed-MD-5, Keyed-SHA-1)

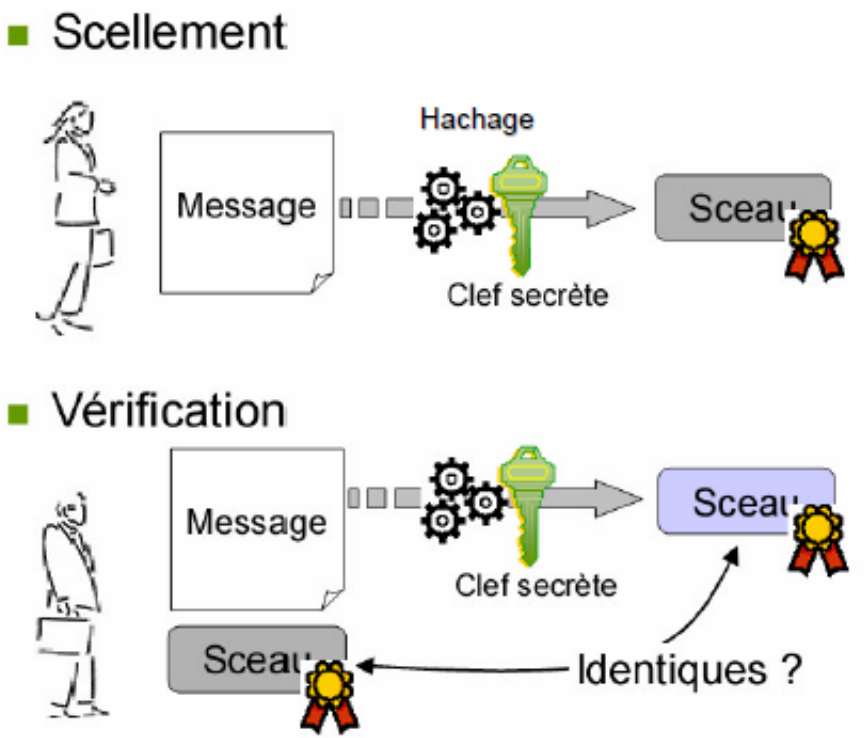


Figure – Scellement

Avantages et Inconvénients des systèmes symétrique

Avantage

- **Algorithmes symétriques sont rapides** (parce qu'ils utilisent de petits entiers et des opérations rapides) ;

Inconvénients

- **Confidentialité de la clé sécrète :** problème de partage de la clé à travers un canal sûr et problème de stockage de la clé ;
- **Durée de vie des clés assez courte.**
- Problème d'authentification

Cryptographie Asymétrique

- Dans le cas des **systèmes symétriques, on utilise une même clé pour le chiffrement et le déchiffrement** ;
- **Problème** repose dans la **transmission de la clé** : il faut que les l'**expéditeur et le destinataire** se **voient** en avance d'abord pour **échanger la clé secrète** ;
- C'est **à partir de ces problemes que les principes du chiffrement asymétrique sont nés** ou ces mis au point ont été **mis par Diffie et Helman en 1976** ;
- Ils ont dégagé la notion de **fonction à sens unique** ;

- Dans le cas des systèmes **asymétriques,** chaque personne possède **deux clés distinctes (privée et publique)** avec impossibilité de **déduire** la **clé privée** à partir de la **clé publique** ;
- De ce fait, il est **possible de distribuer librement la clé publique ;**
- Il existe trois grands usages de la cryptographie asymétrique :
  - **Le chiffrement asymétrique** ;
  - **Les signatures numériques** ;
  - **L'échange de clés**.

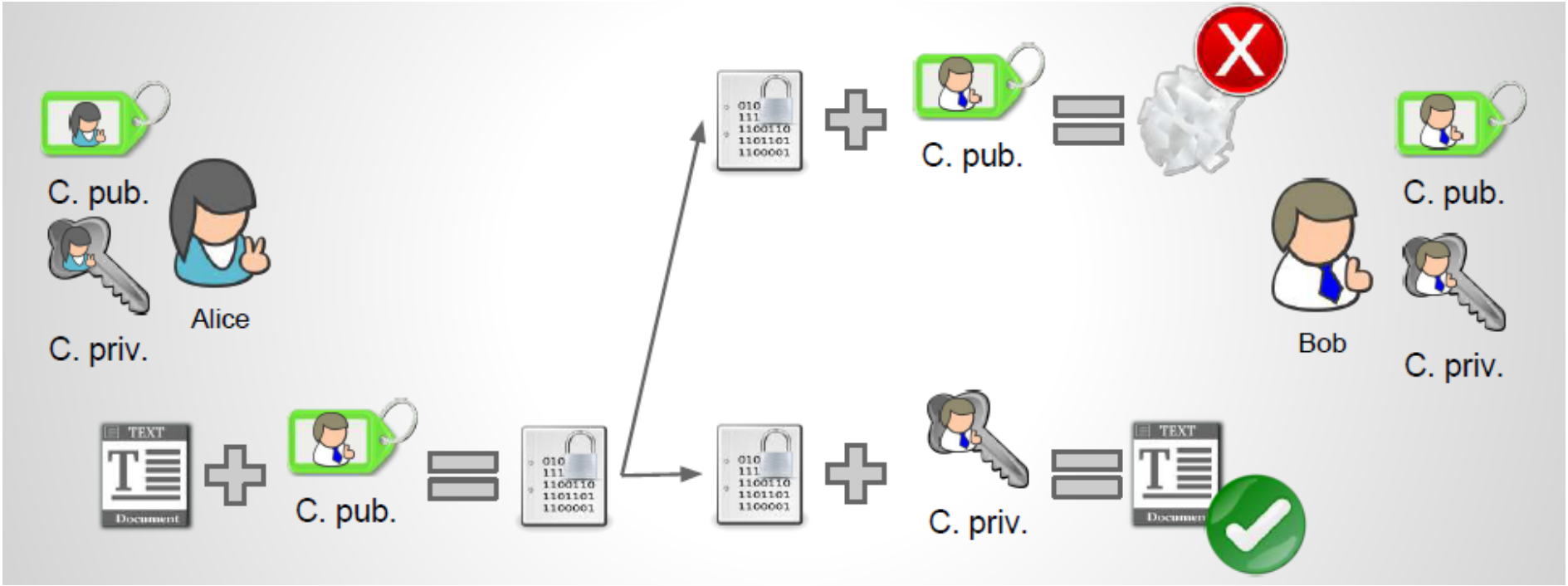


Figure – Schema du système asymétrique

Quelques Algorithmes à clé publique

Exemples

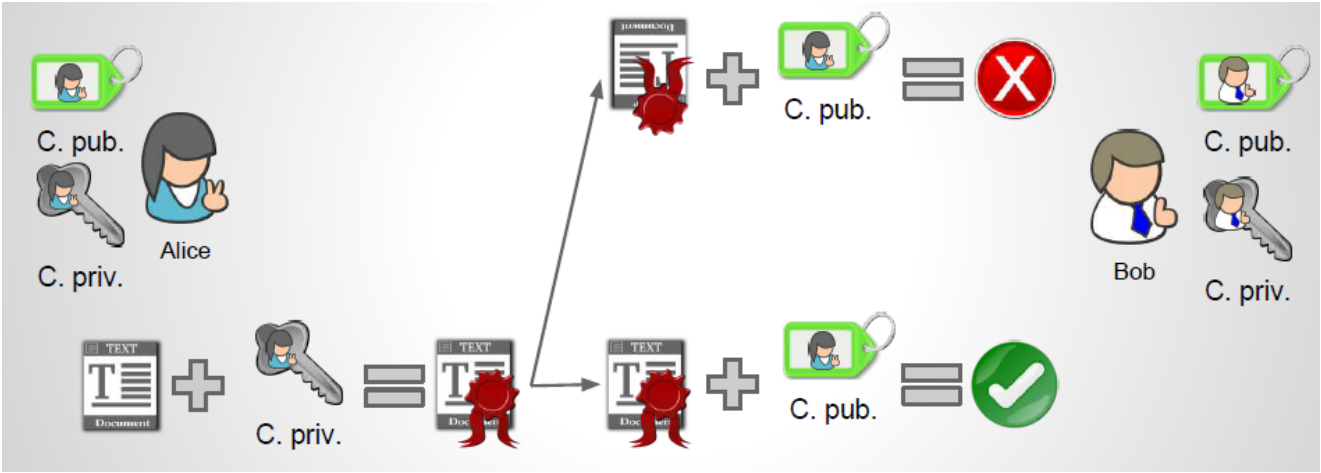
- **Rabin**(Chiffrement) : factorisation de grands entiers ;
- **ElGamal** (chiffrement) : logarithme discret ;
- **Merkle-Hellman**(Chiffrement) : problème de la somme de sous-ensembles (un cas spécial du problème du sac à dos) ;
- **NTRU :**(Chiffrement) problème sur les réseaux arithmétiques .
- **RSA**(chiffrement, signature) : factorisation de grands entiers ;
- **DSS/DSA**(signature, pouvant utiliser ElGamal. . .) ;
- **Diffie-Hellman** (échange de clé) : logarithme discret ;

Longueur de clé

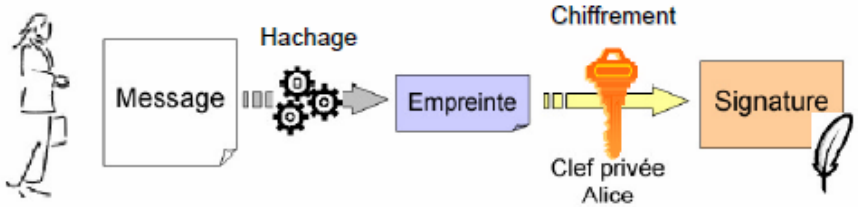
- La **recherche des clés par force brute est toujours théoriquement possible mais les clefs utilisées** sont trop grandes **($>$ 1024 bits)** ;
- Par exemple le module **RSA est à 2048 bits** actuellement.

Signature numérique

- Une signature (digitale-manuelle ou numérique-cryptographique) est un **procédé, qui, appliqué à un message, garantit la non répudiation** par le **signataire**
- Elle doit posséder les **propriétés suivantes :**
  - **Unique**
  - **Impossible à usurper**
  - **Impossible à répudier par son auteur,**
  - **facile à vérifier par un tiers,**
  - **facile à générer**



- Signature



- Vérification

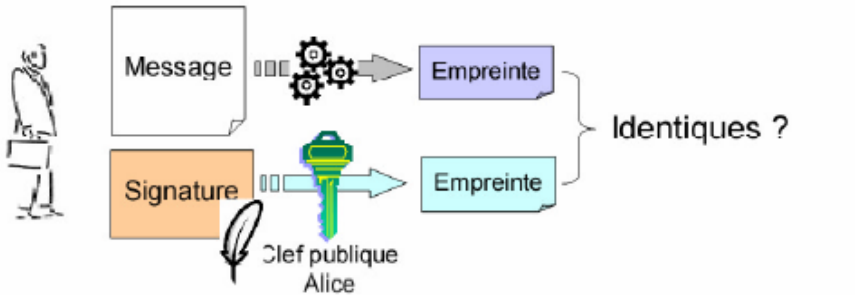


Figure – Signature numérique

Comparaison des signatures numérique et manuelle

Signature manuelle

- **Associé physiquement au document** signé ;
- **Identique pour tous les documents** venant d'un même signataire ;
- Habituellement à la **dernière page.**

Signature numérique

- Peut être **stockée et envoyée indépendamment** du document signé ;
- **Couvre l'entièreté du document**

Algorithme de chiffrement et signature

RSA

1. **Algorithme de génération des clés**
   - Générer aléatoirement 2 grands nombres premiers p et q
   - Calculer $n = P \times q$
   - Calculer $\varphi(n) = (P-1)(q-1)$
   - Choisir un entier **e** vérifiant $0 < e < \varphi(n)$ et $\text{pgdc}(e, \varphi(n)) = 1$
   - Trouver un **d** tel que $0 < d\varphi(n)$ et $ed \equiv 1 mod \varphi(n)$
   - Clé publique est constituée de **e**(l'exposant publique) et **n** (le module)
   - Clé privée est constituée de **d** (l'exposant privé) et **n**.
   - Clé publique RSA : (n, e)
2. **Algorithme de chiffrement**

- Message **m**, $1 \leq m \leq n-1$
- Message chiffré : **c**, $c = m^e \bmod n$

Algorithme de déchiffrement

- Message déchiffré : **c**
- Clé privée RSA : (n, d)
- Message retrouvé : **m,**

$$m = c^d \bmod n$$

Algorithme de signature

- Alice crée sa signature numerique en utilisant

$$S = m^d mod n$$

  ou **M est le message**
- Alice envoie le message M et la signature S à Bob
- Bob Calcule

$$m_1 = S^e mod\ n$$

- Si $m_1 = m$ alors Bob accepte les données envoyé par Alice

Rabin

- Choisir **deux grands nombres** premiers, p et q, au hasard ;
- Posons n = pq, ce qui fait de n la **clé publique**.
- Nombres **premiers** p et q constituent la **clé privée** ;
- **Chiffrer**, on n'a besoins que de la **clé publique**, n.
- **Déchiffrer**, les facteurs de n, p et q, sont nécessaires.

1. **Algorithme de chiffrement**
   - Texte chiffré c se détermine comme suit.
   $$c = m^2 mod n.$$
   - Autrement dit, c est le **résidu quadratique du carré du texte en clair** , pris **modulo n**.
2. **Algorithme de déchiffrement**
   - Racines carrées
   $$m_p = \sqrt{c} \text{ modp et } m_q = \sqrt{c} \text{ moq sont calculées}$$
   - Algorithme d'Euclide étendu permet de calculer y_p et y_q, tels que :
   $$y_p.p + y_q.q = 1$$

ElGhamal

1. **Algorithme de génération des clés**
   - Choisir G un **groupe** et $g \in G$ d'ordre q, (n = Card G $\geqslant$ 124, |q| $\geqslant$ 160, q divise nplp)
   - Alice choisit a aléatoire dans $]1, n-1[$ et calcule $h = g^a$ dans G(|a|=|q|)
   - Clé publique est (g, h G)
   - Clé secrète est a.
2. **Algorithme de chiffrement**
   - Clé publique est (g, h,G) ;
   - Choisir un nombre aléatoire $k \in]1, n-1[$ assez grand (|a|=|q|)
   - Pour chiffrer un message clair m, Bob calcule :
     - $m_1 = g^k \in G$
     - $m_2 = m.h^k \in G$
     - Chiffré c = (m1,m2).
3. **Algorithme de déchiffrement**
   - Clé privée a ;
   - Alice reçoit le chiffré c = (m_1, m_2) ;
   - Elle calcule : $m^{'} = m^{p-1-a}.m_2 \in G$

Algorithme de signature

- Alice souhaite signer un document M ;
- Elle choisit au hasard un entier $]1, n-1[$ tel que pgcd(k ; p - 1) = 1 $\Longleftrightarrow k^{-1} \in G$ existe ;
- Signature de M : s(M) = (r ; s) avec
  - r = g^k
  - s = $k^{-1}(M - a.r)$mod(n-1)
  - Le document signé est alors [M ; s(M)].

Algorithme de vérification

- La signature est dite valide si
  - 0 <r < n
  - $h^r r^s = g^M$(modn)

DSA-domaine

1. Choisir un nombre premier **q** vérifiant : $2^{159} < q < 2^{60}$
2. Choisir un entier **t** : $0 < t < 8$
3. Choisir un nombre entier **P** vérifiant : q divise P - 1 et $2^{511+64t} < P < 2^{512+64t}$
4. Choisir un entier g d'orde q
   - 4.1. Choisir un entier $h \in [1, P-1]$
   - 4.2. Calculer g $= h^{(P-1)/q}$ mod P
   - 4.3. Si $g = 1$ alors retourne à 4.1.
5. Retourner (P, q, g)

Protocoles d'échange de clés

- En **informatique**, et plus particulièrement en **cryptologie**, un protocole d'échange de clé (ou de **négociation de clé, ou de distribution de clé**)
- Est un **mécanisme** par lequel **plusieurs participants** se mettent d'**accord sur une clé cryptographique**
- Il existe **deux types de protocoles d'échange** de clés :
  - Protocoles qui supposent le partage préalable d'une information (clé publique) entre les des 2 entités (ex. RSA utilisé par HTTPS)
  - Protocoles qui supposent aucune connaissance préalable d'informations entre les 2 entités (ex. Diffie-Hellman)

Protocole d'échange de clés : ex. RSA

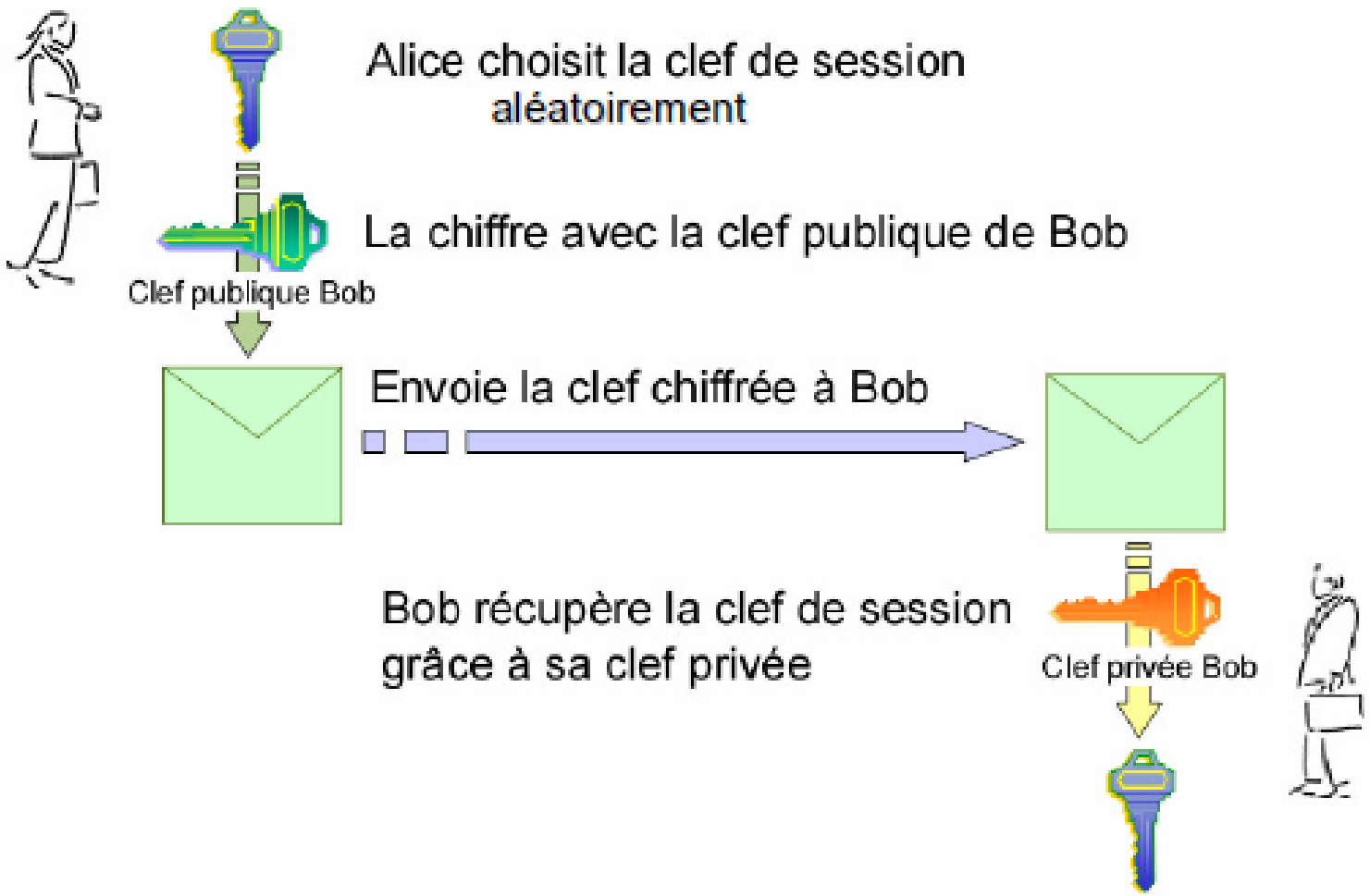


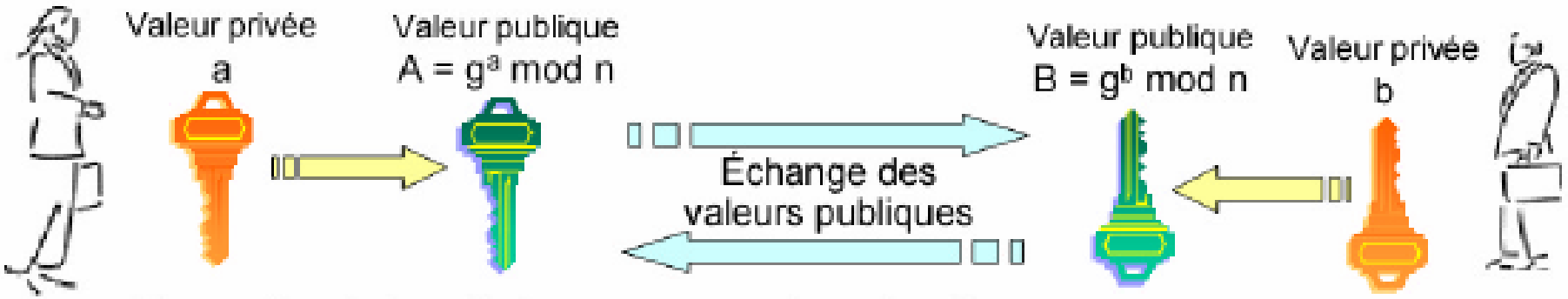
Figure – Protocole d'échange de clés : ex. RSA

Protocole d'échange de clés Diffie-Hellman

- Pour que Alice et Bob échangent une clé, ils s'entendent d'abord sur un **groupe** G (noté multiplicative)
- Ils fixent publiquement un p premier et un entier g dans G puis **effectuent les étapes** suivantes :
  - **Alice et Bob** choisissent un **élément** g **d'ordre premier suffisamment grand dans** G ;
  - **Alice** choisie un **parametre secret** (valeur aléatoire $a < p$)et calcule A= g^a dans G et transmet **publiquement** g^a à **Bob** ;
  - **Bob** choisie un **paramètre secret** (valeur aléatoire $b < p$) et **calcule** B= g^b dans G et **transmet publiquement** g^b à **Bob** ;
  - **Chacun deux calcule** la valeur commune $k = (g^b)^a = (g^a)^b$ qui constituera leur **clé privé** ou comme **outil pour fabriquer la clé privée**.
  - L'espion **Charlie** qui **suit la communication** connait A, B, g, p, g^a, g^b **ne doit pas pouvoir calculer** $k = (g^b)^a = (g^a)^b$
  - Ce problème est basé sur le logerithme discret mais reste moins difficle en théorie.

Échange de clés Diffie-Hellman

- Échange de valeurs publiques



- Permettant de générer un secret partagé

Figure – Protocole de Diffie-Hellman

Certificat électronique

Concept

- Nous avons **décrit les mécanismes** qui permettent d'**assurer la sécurité avec le couple de clé publique et les algorithmes de chiffrement** asymétriques ;
- Mais il ya une **énorme oublie** dans les raisonnements précédents :
- On a considéré qu'un **utilisateur prenait connaissance de clé publique** d'une personne simplement en consultant un **annuaire(ou un serveur web)** ;
- Mais qu'est ce qui **garantit que la clé publique de Bob que l'utilisateur a ainsi récupérée est la bonne ?**
- Un pirate, **Remane** peut par exemple remplacer la clé publique de **Bob** par la sienne

- Une fois cette **mascarade commise, Remane** pourra **lire les courriers confidentiels** destiné à **Bob** et **signer des messages** en se faisant passer pour **Bob**
- Il a donc fallu **créer un mécanisme supplémentaire** pour pouvoir **vérifier la validité d'une clé publique :** C'est le **rôle des certificat ;**
- Un **certificat électronique ou numérique d'une personne** est l'équivalent électronique d'une **carte d'identité ou d'un passeport.**
- Un **passeport contient** des **informations concernant le propriétaire (Nom, prénom, adresse, etc), la signature manuscrite, la date de validité ainsi qu'un tampon et une présentation (forme,couleur,papier)** qui permettent de reconnaitre que ce passeport n'est pas un **faux** qu'il a été **délivré par une autorité bien connue ;**
- Le **certificat électronique est un petit fichier** qui contient des informations similaire.

- Les **deux formats les plus utilisés** aujourd'hui sont :
  - X.509, défini dans la RFC(Request For Comments) ;
  - OpenPGP, défini dans la RFC .
- C'est un **petit fichier,** qui contient au **moins les informations suivantes** :
  - Le nom de l'autorité (de certification) qui a créé le certificat
  - Le nom et le prénom de la personne
  - Son entreprise (CNRS par exemple)
  - Son service (au CNRS, le nom du laboratoire)
  - Son adresse électronique
  - Sa clé publique
  - Les dates de validité du certificat
  - Des informations optionnelles
  - Une signature électronique

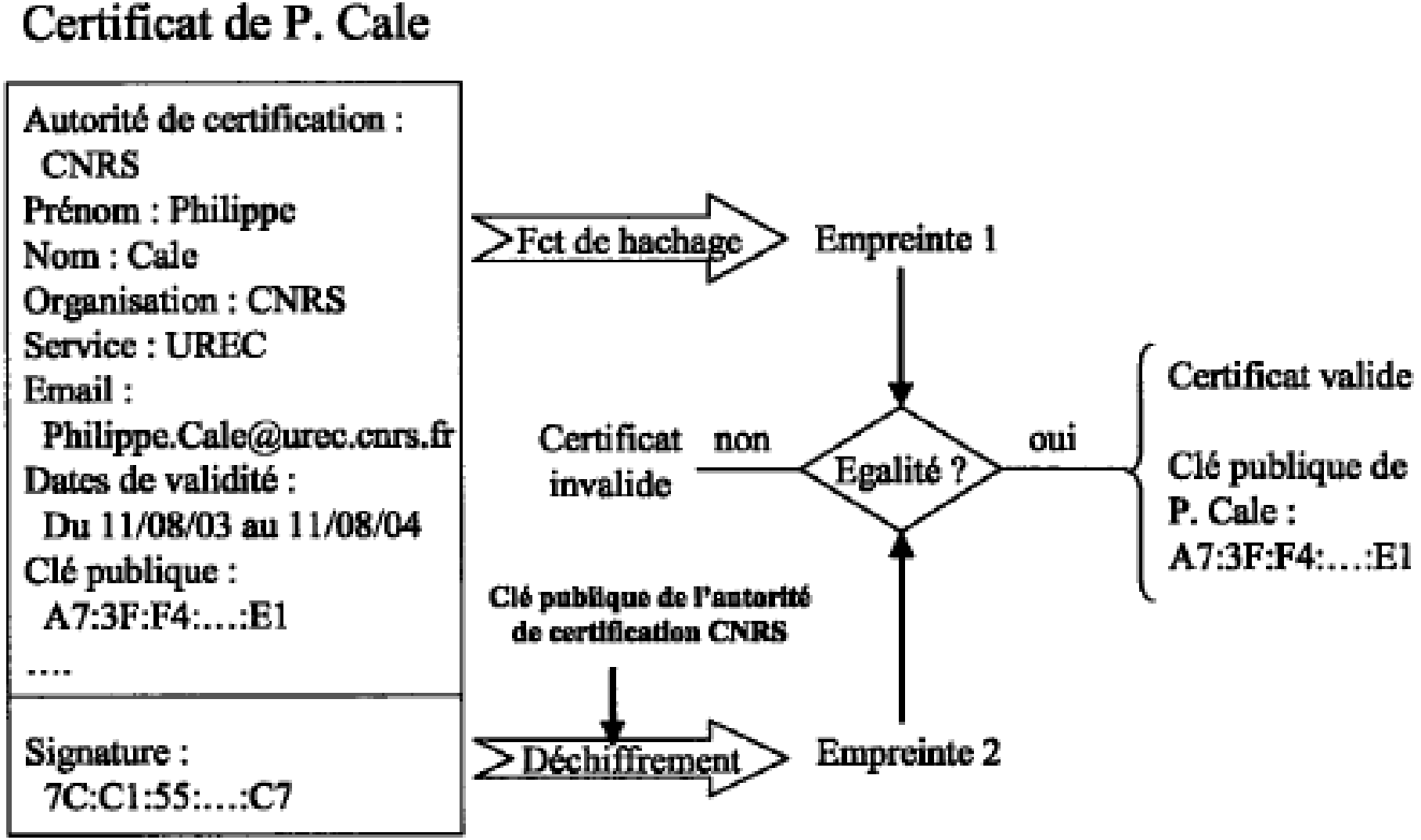


Figure – Certificat numérique

Types de certificats

- Le **type de certificats électroniques** dépend du support qui l'héberge. Ainsi, nous pouvons distinguer trois types de certificats :
  - **le certificat serveur((Serveur web) (voir TLS et X.509)**
  - **le certificat personnel ou client**
  - **le certificat IP SEC (Internet Protocol Security) ou VPN**

Autorité de certification et infrastructure de gestion de clés

- Définition d'une autorité de certification
  - Une **autorité de certification (AC)** est un **organisme reconnu** comme étant **compétent** pour délivrer des **certificats à une population** auprès de laquelle elle a toute **confiance et en assurer la validité.**
  - Elle s'engage sur l'identité d'une personne au travers du certificat électronique qu'elle lui remet.
  - La confiance que l'on accordera à un certificat va dépendre du sérieux de l'autorité qui l'aura délivré.
  - **Le choix de l'autorité de certification dans une organisation ou une entreprise est une décision stratégique.**

- **Infrastructure de gestion de clé**
  - Quelle que soit **l'autorité de certification** choisie, il faut définir ce que l'on appelle une **architecture de gestion des certificats**.
  - **Infrastructure de Gestion de Clés(IGC)** et **Public Key Infrastructure(PKI)** sont les deux sigles les plus connus pour la désigner.

- L'utilisation des systèmes à clé publique :
  - à grande échelle, nécessite des systèmes complexes appelés **PKI (Public Key Infrastructure)** .
  - à petite échelle, nécessite une chaine de confiance à défaut d'un **PKI** : c'est le cas de l'Utilisation de **Gnu-PG (voir TP)** pour le chiffrement des mails sur internet

Cryptographie hybride

Concept

- **Cryptographie asymétrique** est intrinsèquement lente à cause des calculs complexes qui y sont associés
- Alors que la **cryptographie symétrique** brille par sa rapidité.
- Toutefois, cette dernière souffre d'une grave lacune de partage de clé d'une maniere sécurisée.
- Pour pallier ce défaut, on recourt à la **cryptographie asymétrique** qui travaille avec une paire de clés(Publique et privée).
- Cryptographie hybride combine les **deux systèmes** afin de bénéficier la **rapidité** de la **cryptographie symétrique** pour le **contenu du message** et utilisation de la **cryptographie asymetrique** uniquement pour la **clé.**
- Cryptographie hybride est un système de cryptographie faisant appel aux deux grandes familles de systèmes cryptographiques.

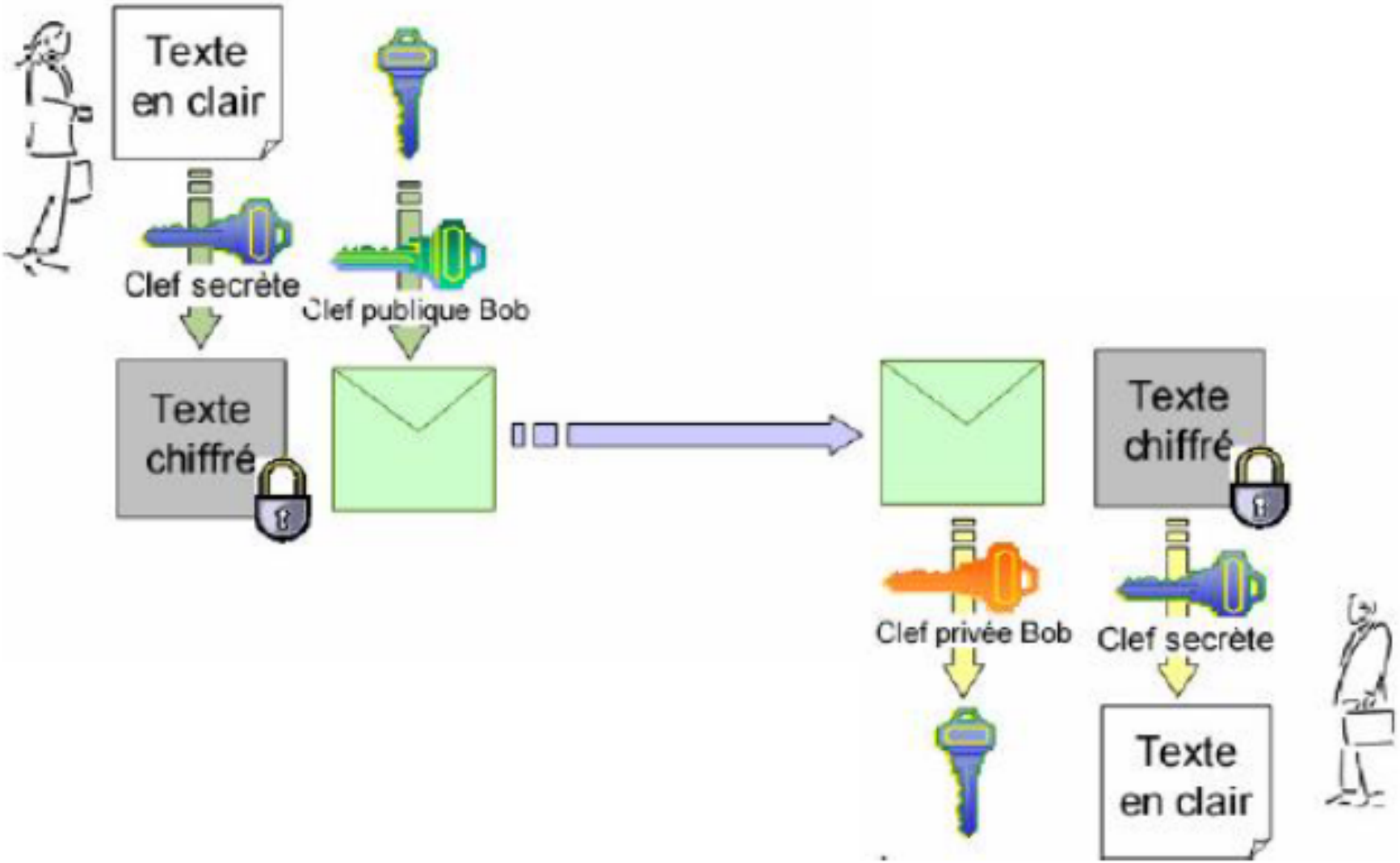


Figure – Schema hybride

Avantage et Inconvénient des systèmes Asymétrique

Avantage

- Le **problème du canal sûr** de communication est résolut ici

Inconvénients

- On garde la **clé privée sur un ordinateur ou une clé USB appelée Token**(Problème de confidentialité) ;
- On **publie la clé publique dans ce qu'on appel un annuaire**(Problème de l'intégrité de la clé publique) ;
- Les **algorithme** asymétriques sont **lents** .

Métiers liés à la sécurité et Mission d'un ingénieur sécurité

Métiers liés à la sécurité

- **Technicien sécurité**
  - Gère la sécurité du réseau et des postes clients sous la supervision d'un ingénieur
- **Ingénieur sécurité**
  - Technicien sécurité plus avancé
- **RSSI**
  - Responsable Sécurité des Systèmes Informatiques
  - Définit la stratégie globale de sécurité d'un réseau d'entreprise et du respect des normes de sécurité
- **DSI**
  - Directeur des Systèmes Informatiques
  - Intégrer la sécurité dans un système d'information global et dans le plan stratégique de l'entreprise

Mission d'un ingénieur sécurité

- **Offre vue sur Internet**
  - Garantir la sécurité des données
    - Sécurité des périphériques et des données (cryptographie)
  - Effectuer des audits de sécurité
    - Auditer l'architecture de sécurité
    - Auditer les protocoles, les services
  - Proposer une stratégie de sécurité
    - Règles d'identification, d'authentification, d'autorisation et de maintenance,
    - Gestion du plan de reprise et de documentation
- **Evaluer les vulnérabilités des systèmes**
  - Tests d'intrusion