

Information, Calcul et Communication

Module 3 : Systèmes

Leçon III.4 : Sécurité de l'Information, de la Communication et du Calcul

préparée par Prs. Ph. Janson & W. Zwaenepoel

Objectifs du cours d'aujourd'hui

Comment sécuriser le monde numérique ?

- ▶ En quoi et comment les systèmes informatiques et leur contenu sont **menacés** et **menacent** indirectement les individus dans leur sphère privée ?
- ▶ Quels sont les principes de base à respecter et les **mécanismes** fondamentaux à déployer pour **protéger** l'information, les systèmes qui la traitent, et les réseaux qui la transportent ?
- ▶ Quelles sont les principales **règles de bonne conduite** des utilisateurs et administrateurs de systèmes informatiques pour se protéger contre les hackers et leurs maliciels ?

Motivation – L'univers numérique doit être sécurisé tout comme le monde physique



Les **affaires** se traitent de plus en plus en ligne

...



... donc de plus en d'**argent et de pouvoir** passent par Internet



... donc **criminalité** et conflits politiques se déroulent de plus en plus en ligne

... car ils suivent toujours argent et pouvoir



Plan de la leçon

- ▶ Principes de base
 - ▶ Menaces et Défenses
 - ▶ Exemple d'équilibre : cas de la destruction/perte
- ▶ Confidentialité, intégrité et responsabilité : cryptographie
- ▶ Authentification
- ▶ Autorisation
- ▶ Règles de bonne conduite
- ▶ Résumé / Vue d'ensemble

Principes de base

- ▶ **La sécurité totale n'existe pas** plus dans le monde informatique que dans le monde physique
- ▶ Dans les deux cas elle est
 - ▶ Une course aux armements entre mécanismes d'attaque et de défense
 - ▶ Un **compromis** entre le **risque** d'une attaque et le **prix** de la défense
- ▶ Comme dans toute situation de défense, les attaques visent les **maillons faibles**
 - ▶ Généralement entre le terminal et le siège (utilisateurs ou opérateurs des systèmes informatiques)
- ▶ **L'éducation** des utilisateurs et des opérateurs est donc essentielle
 - ☞ C'est le but de cette leçon !

Les menaces – Leurs objectifs

► Les informations

⇒ Les applications qui les gèrent

⇒ Les logiciels qui les hébergent

⇒ Les ordinateurs qui les exécutent

⇒ Les réseaux qui les relient

⇒ Les bâtiments qui les renferment

⇒ Les utilisateurs & les personnes concernées

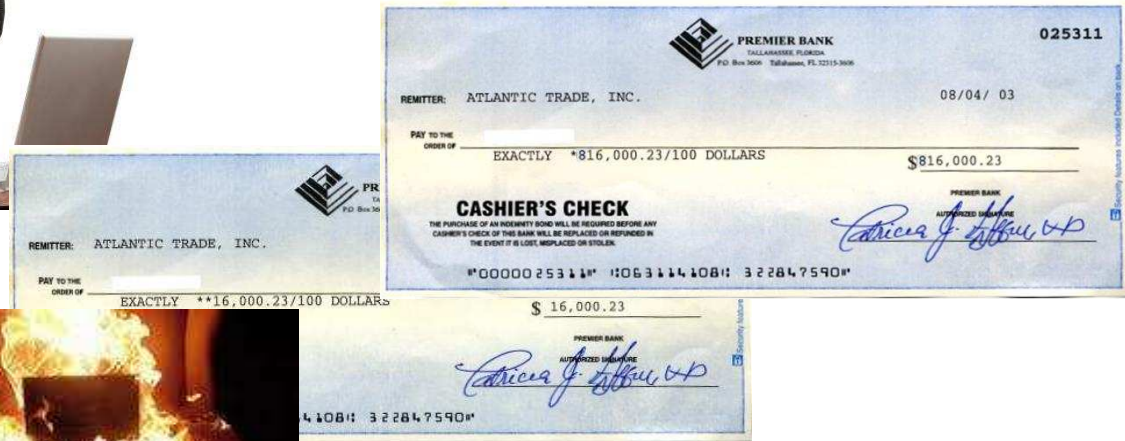
Sécurité de l'Information	Sécurité des Communications		Sécurité du Calcul
Menaces	Défenses	Sécurisation	Sphère privée

Les menaces – Leurs intentions

► Le vol



► La manipulation



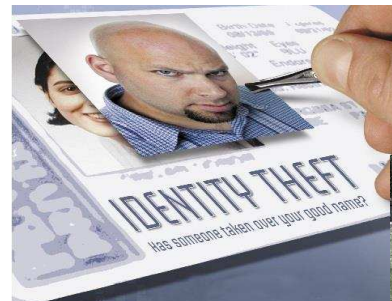
► La destruction



► Le démenti



► L'usurpation d'identité



► Le contournement de défenses



Sécurité de l'Information	Sécurité des Communications	Sécurité du Calcul
Menaces	Défenses	Sécurisation
		Sphère privée

Les menaces – Leurs sources

► Environnementales

- Catastrophes naturelles

► Humaines

▪ Internes

- Les erreurs
- Les abus de privilèges (par des personnes autorisées)

▪ Externes

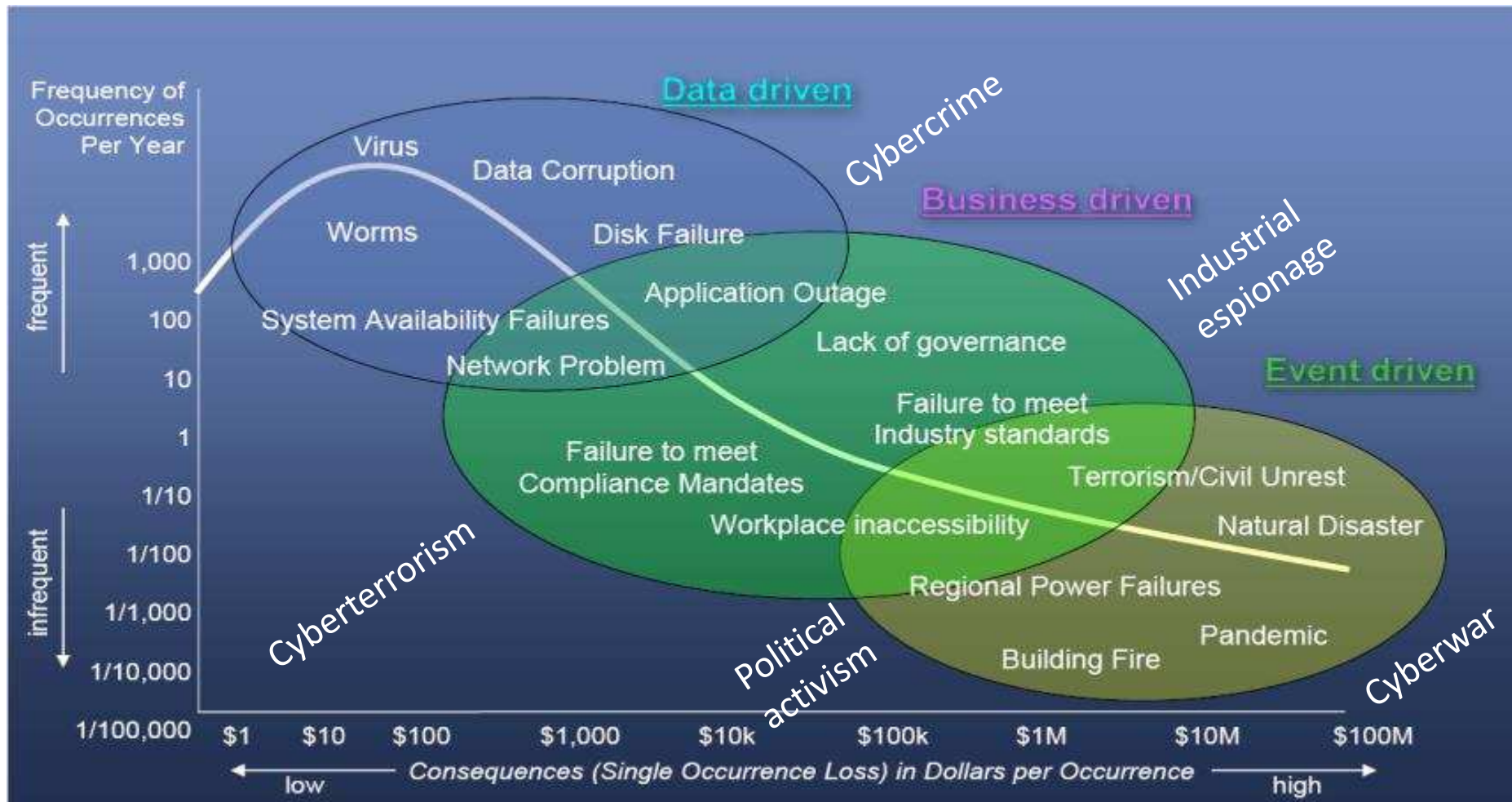
- La manipulation sociale (abus de confiance, mensonge, tromperie, corruption, etc.)
 - Par mail ou web
 - Par réseaux sociaux
- Les attaques physiques (espionnage, vol, sabotage, destruction, etc.)

► Techniques

- Les attaques informatiques par des pirates
 - Par exploitation de vulnérabilités logicielles (“bugs” = coquilles)
- Les maliciels = logiciels malveillants (virus, vers, chevaux de Troie, etc.)
 - Les chaînes de production contaminées

- NB: des accidents de nature environnementale sont souvent source d’abus de nature humaine et d’attaques de nature technique

Les menaces – Leur réalité et leur ampleur



Les menaces – Leur réalité et leur relativité

- ▶ Coût annuel de la cybercriminalité \$ 1 T (10^{12}) (attribué à McAfee)
- ▶ Nombre de vulnérabilités logicielles > 60 K (IBM)
- ▶ Nombre de maliciels identifiés 50-100 M (Webroot)
- ▶ Nombre de sites web infectés > 500 K (Dasient 2010)
- ▶ Nombre de pages web infectées > 5M (Dasient 2010)
- ▶ Taux de spam ~ 90%
- ▶ Comptes Facebook corrompus ~ 15M / 1B (= 1.5%)
- ▶ Nombre de téléphones portables perdus par semaine à Londres 25K
- ▶ Nombre d'ordinateurs portables oubliés par semaine dans les aéroports US 12K

- ▶ Le baromètre (gratuit) des attaques Internet
http://www.barometer.interoute.com/barom_main.php
fournit des statistiques en temps réel sur les attaques en cours

▶ Aussi impressionnants que soient ces chiffres absolus, ils indiquent un équilibre relatif entre coût des risques et prix des défenses

Sécurité de l'Information	Sécurité des Communications		Sécurité du Calcul
Menaces	Défenses	Sécurisation	Sphère privée

Défenses : objectifs principaux

L'ultime objectif: Contrôler qui a quel droit

Les menaces étaient

► **Le vol d'informations**

► **La manipulation**

► **La destruction**

► **L'usurpation d'identité**

► **Le démenti**

► **Le contournement de défenses**

Les combattre exige

► Confidentialité

► Intégrité

► Disponibilité

► Authentification

► Responsabilité

► Autorisation



Sécurité de l'Information		Sécurité des Communications		Sécurité du Calcul	
Menaces		Défenses	Sécurisation	Sphère privée	

Sécurisation de l'information

► Méfiez-vous de la **qualité** des données

Erreurs à la saisie ou l'importation
Données périmées ou non purgées

► Méfiez-vous de l'**authenticité** des données

Des outils aident heureusement à détecter le plagiat
(e.g. www.copyscape.com)

⇒ **Attention!**
**Ne croyez jamais tout
ce qu'on trouve sur la toile !**



Plan de la leçon

- ▶ Principes de base
 - ▶ Menaces et Défenses
 - ▶ **Exemple d'équilibre : cas de la destruction/perte**
- ▶ Confidentialité, intégrité et responsabilité : cryptographie
- ▶ Authentification
- ▶ Autorisation
- ▶ Règles de bonne conduite
- ▶ Résumé / Vue d'ensemble

Destruction: Menace / Défense

- ▶ Menace: la perte ou l'indisponibilité des données
- ▶ Défense: la réplication des données

La réplication

► Réplication: maintenir plusieurs copies des données

Le degré de réplication

- ▶ Tenir une seule autre copie sur une autre machine
 - Bien si la machine originelle tombe en panne
 - Pas suffisant si la machine originelle et la réplique tombent en panne

Le degré de réplication

- ▶ Tenir une seule autre copie sur une autre machine
 - Bien si ...
 - Pas suffisant si ...
- ▶ Tenir une deuxième autre copie
 - Bien si ...
 - Pas suffisant si ...
- ▶ Tenir N copies
 - Bien si ...
 - Pas suffisant si ...

La localisation des répliques

- ▶ Mettre la réplique à côté de l'originel
- ▶ Mettre la réplique à distance

La mise à jour des répliques

- ▶ A chaque modification
- ▶ Une fois par jour
- ▶ Une solution intermédiaire: mettre à jour
 - Une réplique “proche” à chaque modification
 - Une réplique “lointaine” chaque jour

Un bel exemple de compromis

- ▶ Entre une défense plus coûteuse
 - N répliques
 - Réplique lointaine
 - Mise à jour instantanée
- ▶ Contre une menace plus grave
 - Panne de N-1 machines
 - Panne ou destruction d'un centre de données
 - Perte de données non-instantanément répliquées

Protection des données – Disponibilité / robustesse



- La perte d'informations varie **entre horreur et catastrophe**
⇒ Leur sauvegarde est un processus essentiel
- On conserve les copies de sauvegarde de préférence **sur un autre site que l'original** pour parer à tout accident qui affecterait le site original dans son ensemble

NB: la préservation pérenne de média extrêmement volumineux est une inconnue
parce que leur **fiabilité** ne peut plus être garantie ($1 \text{ erreur} / 10^9 \text{ bits} = 1000 \text{ erreurs} / 1\text{TB}$)
et qu'une copie complète n'est plus **économique**,
vu que le volume des données augmente chaque année d'un **facteur 4**
alors que la densité des supports n'augmente "que" d'un **facteur 1.5 à 2**

Plan de la leçon

- ▶ Principes de base
- ▶ Confidentialité, intégrité et responsabilité : **cryptographie**
 - ▶ principes
 - ▶ cryptographie à clé privée
 - ▶ principes
 - ▶ exemple du XOR
 - ▶ cryptographie à clé publique
 - ▶ principes
 - ▶ exemple de RSA
- ▶ Authentification
- ▶ Autorisation
- ▶ Règles de bonne conduite
- ▶ Résumé / Vue d'ensemble

Confidentialité: Menace / Défense

- ▶ Menace: lecture non autorisée
- ▶ Défense: la cryptographie

La cryptographie

- ▶ Le cryptage
- ▶ Le décryptage
- ▶ A l'aide d'un secret ou d'une clé




La cryptographie

- ▶ Le cryptage
 - $\text{message crypté} = \text{crypt}(\text{message clair}, \text{clé})$

- ▶ Le décryptage
 - $\text{message clair} = \text{decrypt}(\text{message crypté}, \text{clé})$

- ▶ Les clés peuvent être différentes

Protection des données – Cryptage

Système		Symétrique à clés secrètes	Asymétrique à clés publiques
Exemple		DES, 3DES, AES	DH, RSA, courbes elliptiques
Fonction			
	Confidentialité	Oui, + efficace	Oui
	Intégrité	Oui, + efficace	Oui
	Responsabilité (Signature digitale)	Non	Oui

► Les navigateurs utilisent les deux (indiqué par un icône dans la barre supérieure/inférieure)

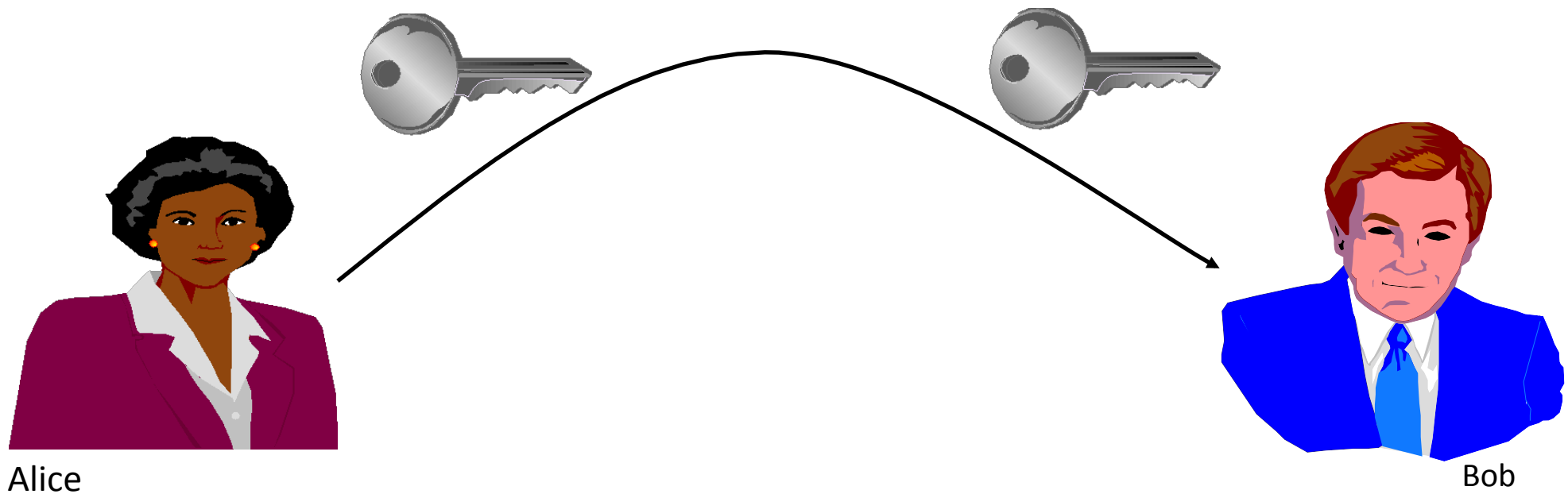


► Le cryptage devrait être **universel**, surtout à l'heure du paradigme du “cloud”

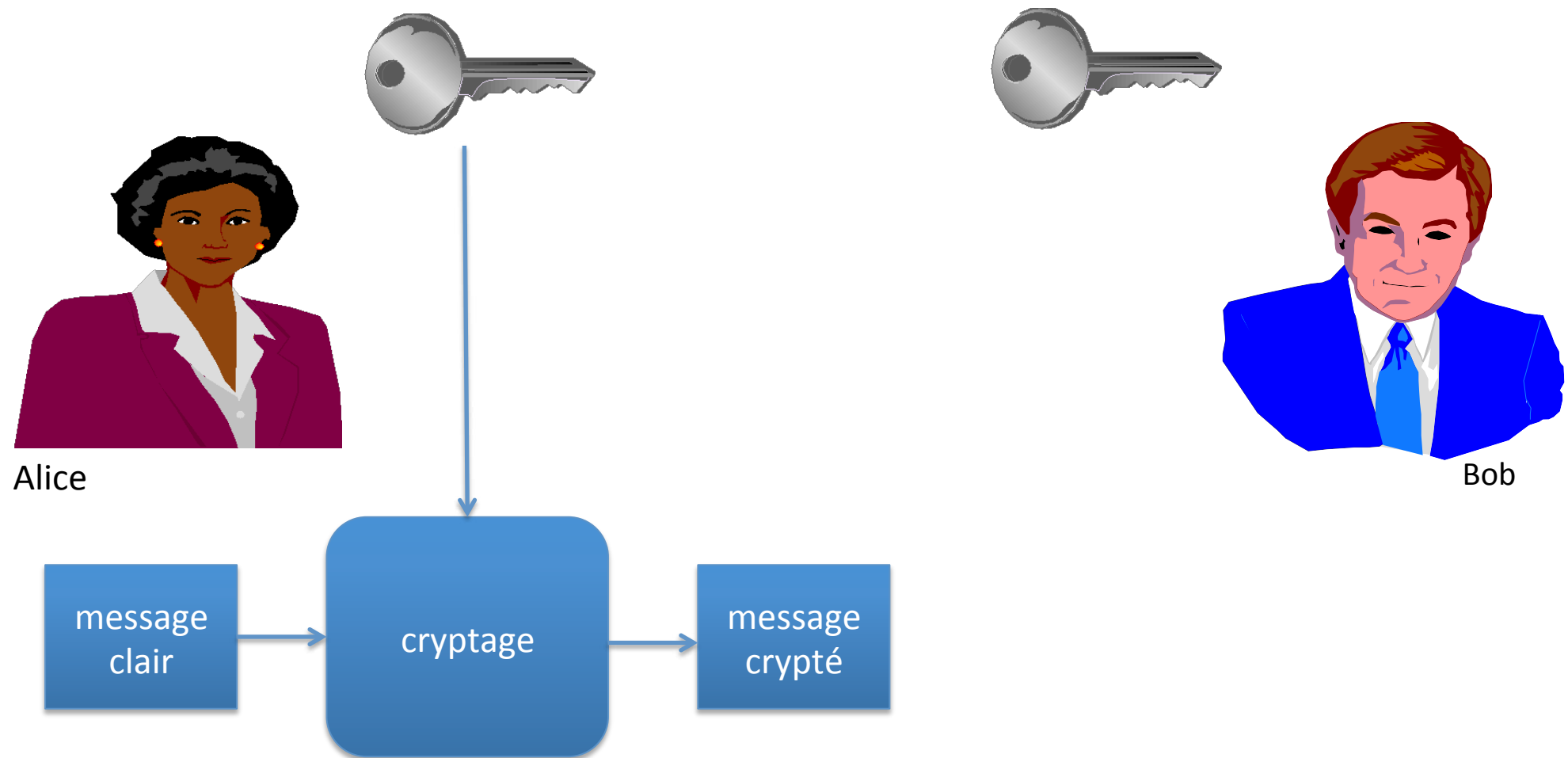
La cryptographie symétrique

- ▶ Il n'y a qu'une seule clé
- ▶ La clé est échangée entre les partenaires en avant
- ▶ Le message est crypté et décrypté avec la même clé

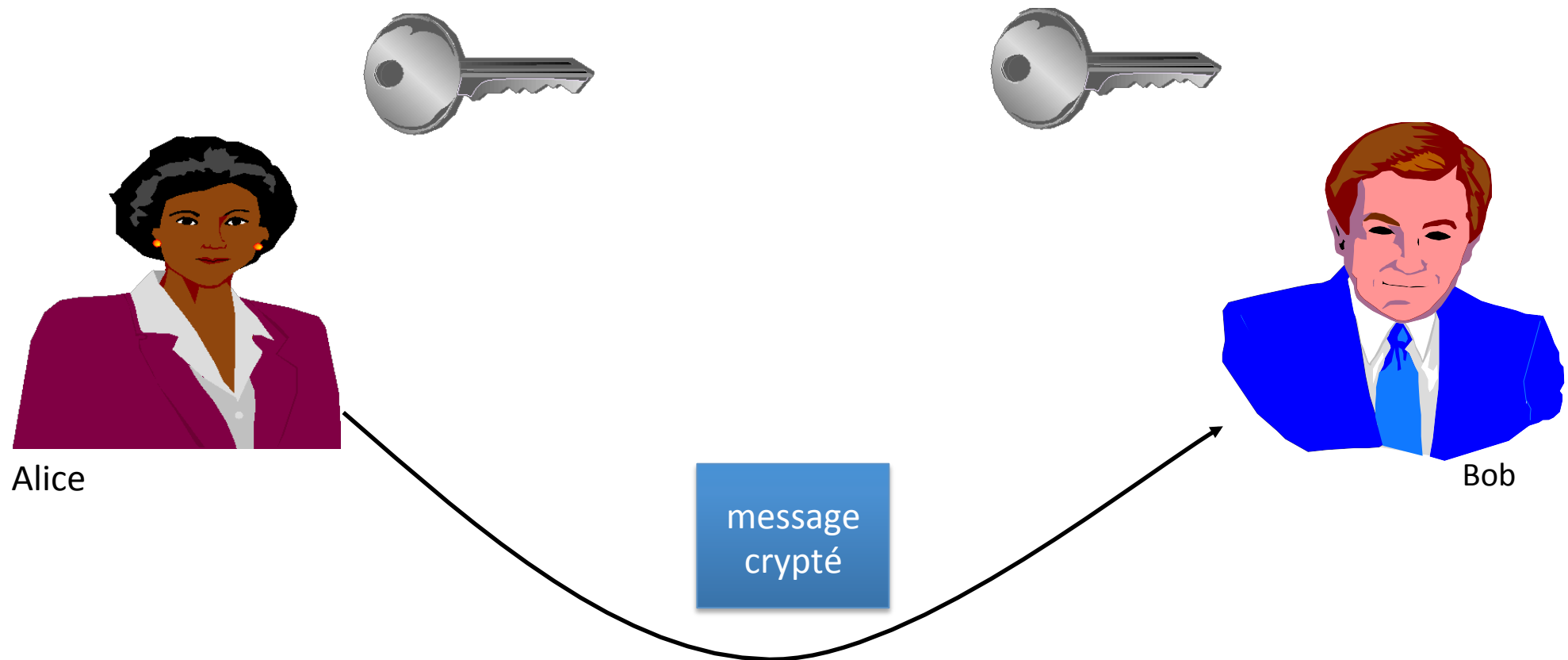
Cryptographie symétrique



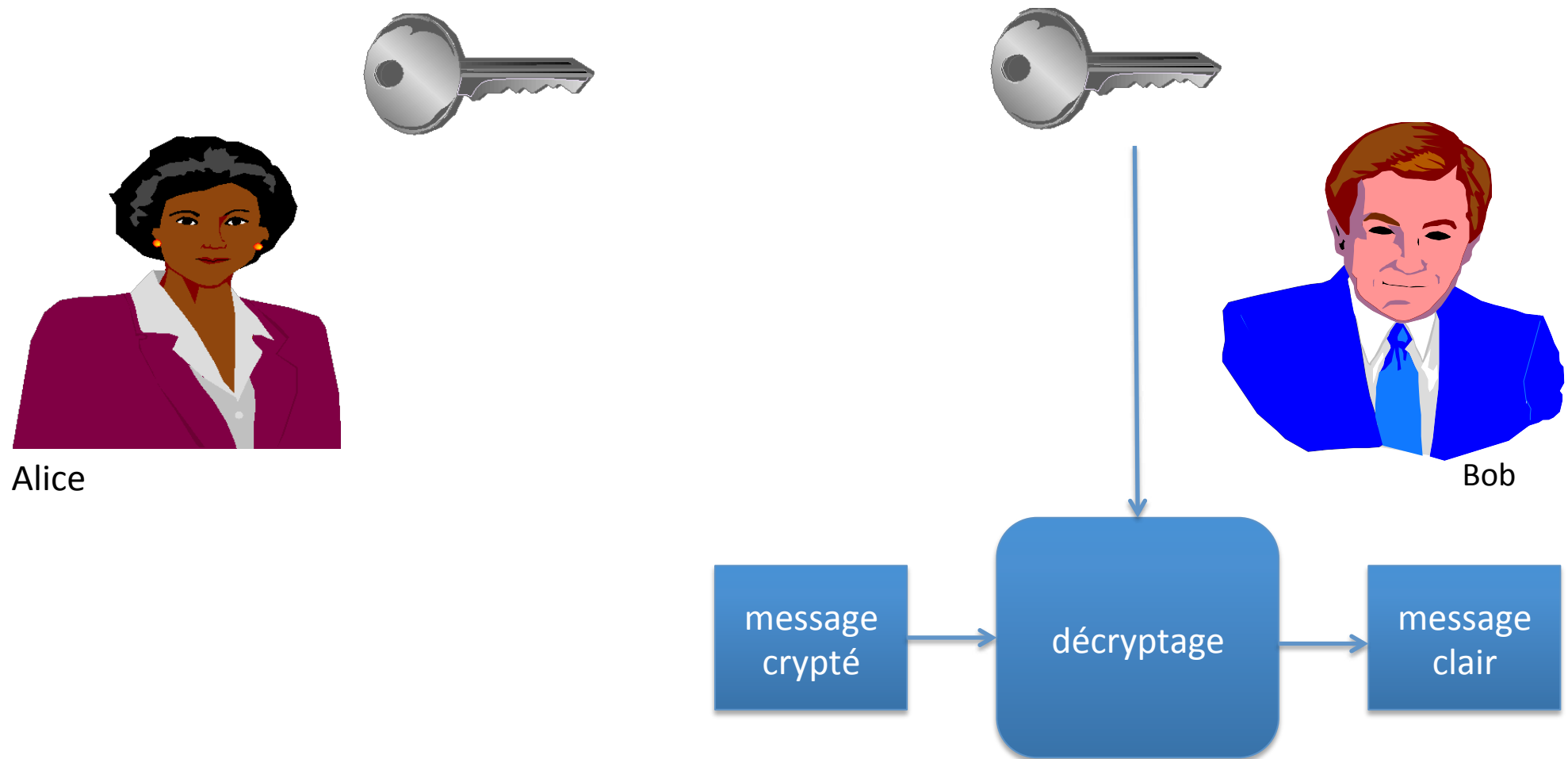
Cryptographie symétrique



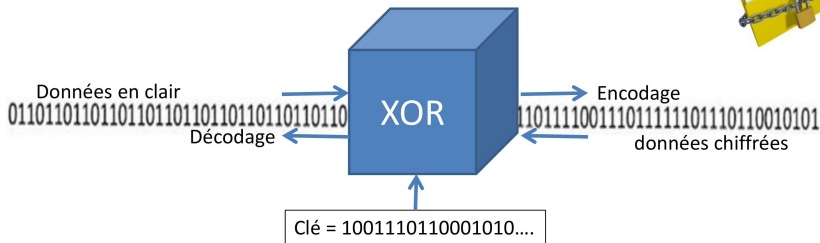
Cryptographie symétrique



Cryptographie symétrique



Cryptage – Exemple : One Time Pad



Les clés secrètes (ou privées) doivent être
"incassables" = ni devinables ni dérivables

Utilise le « OU EXCLUSIF (*XOR*) », bit à bit :

	0	1
0	0	1
1	1	0

Cryptage : principes fondamentaux

Pour être totalement sûr d'un point de vue « théorie de l'Information » un système de cryptage de messages M avec des clés K doit vérifier :

- ▶ la taille des K doit être supérieure ou égale à celles des M
- ▶ l'entropie des K doit être supérieure ou égale à celles des M

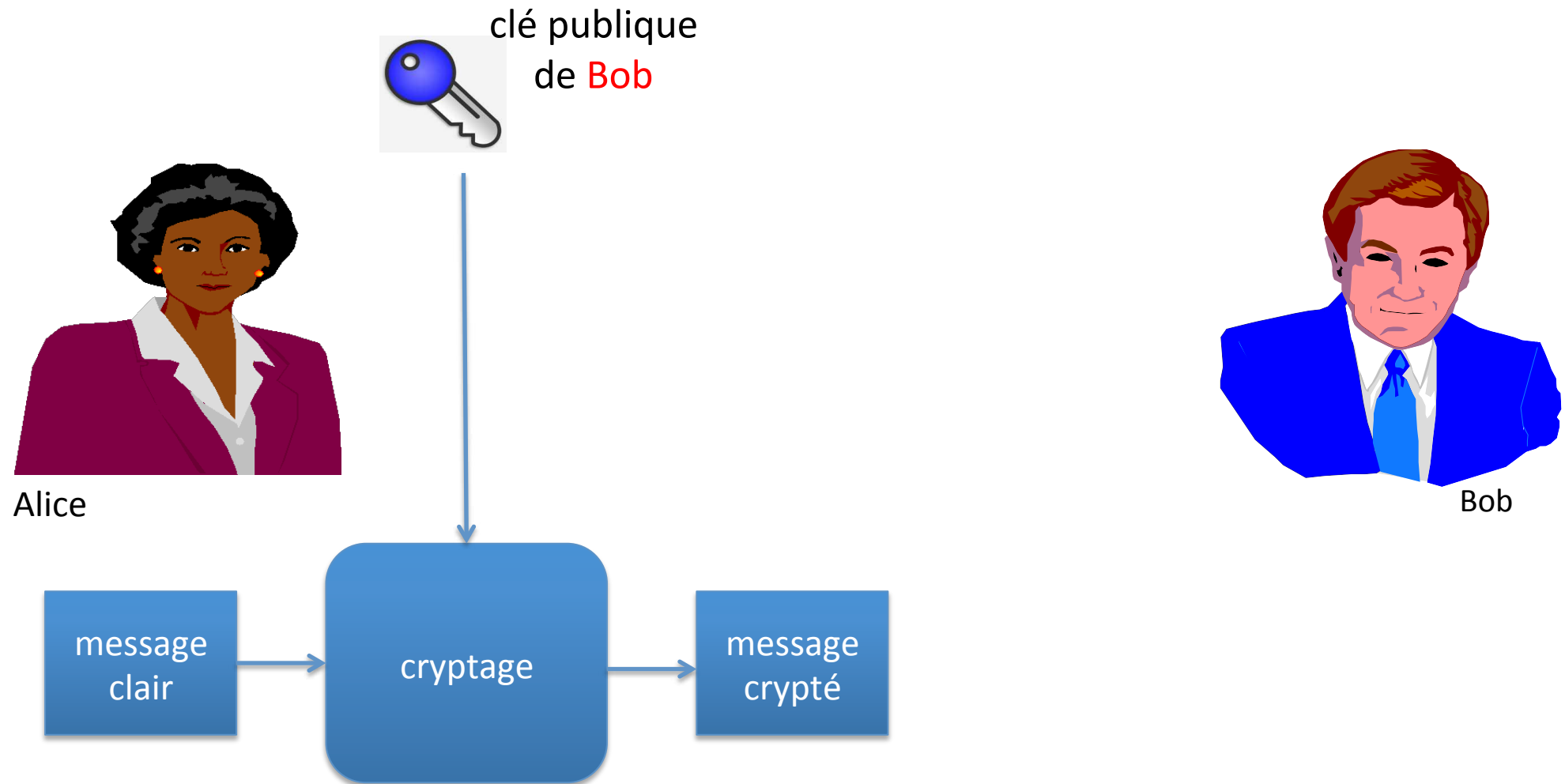
En clair : les clés doivent être « au moins aussi complexes que les messages eux-même »

👉 peu pratique

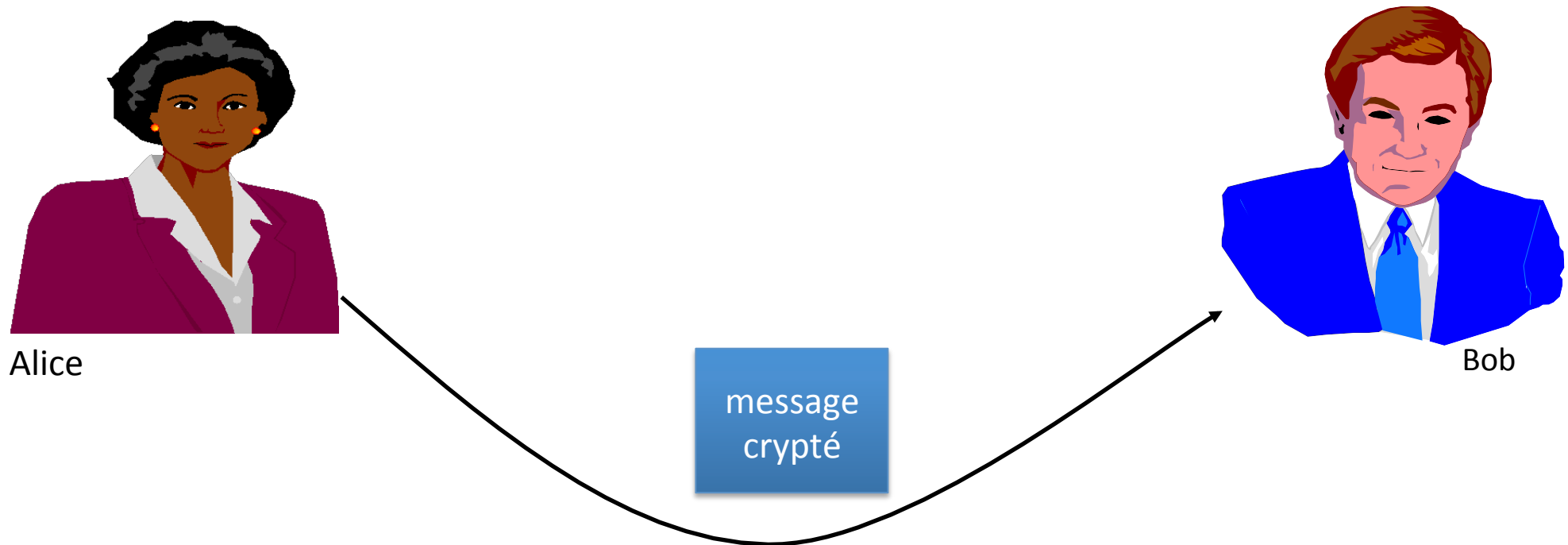
La cryptographie asymétrique

- ▶ Chaque utilisateur a deux clés
 - Une clé privée
 - Une clé publique
- ▶ Le cryptage se fait avec la clé publique du *destinataire*
- ▶ Le décryptage se fait avec la clé privée du destinataire

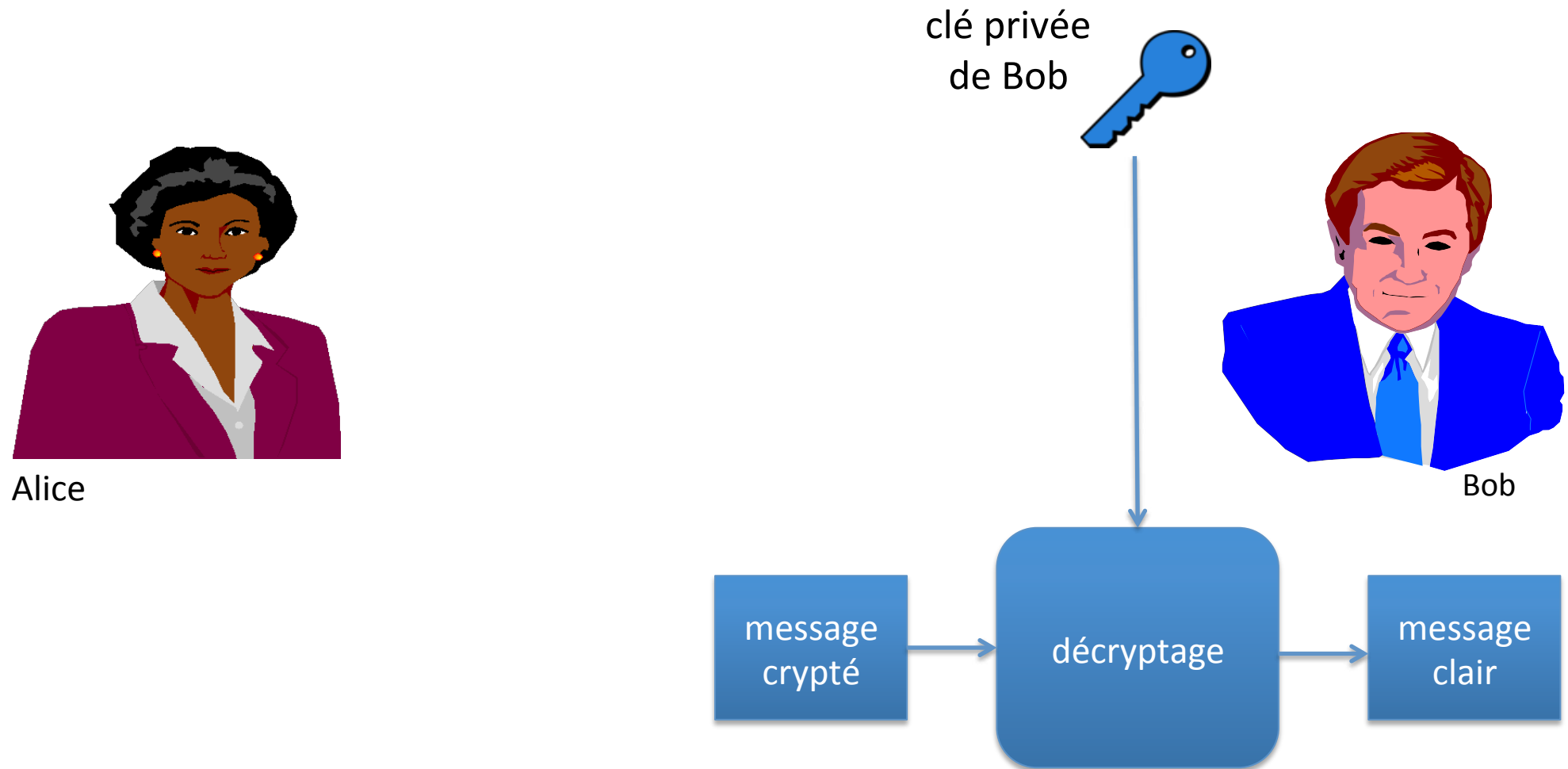
La cryptographie asymétrique



La cryptographie asymétrique



La cryptographie asymétrique



Conditions nécessaires

- ▶ $\text{Decrypt}(\text{crypt}(\text{message}, \text{clé publique}), \text{clé privée}) = \text{message}$
- ▶ Impossible de deviner la clé privée à partir de la clé publique

Exemple – Le principe de RSA

- ▶ Choisir m et n premiers (> 300 chiffres décimaux) tels que tout message $M < m \cdot n$
 - ▶ Calculer $x = m \cdot n$, $c = (m-1) \cdot (n-1)$
 - ▶ Choisir comme clé publique
 P premier avec c (et inférieur à c)
 - ▶ Dériver comme clé privée
 S tel que $SP = 1 \text{ mod}(c)$
 - ▶ Oublier / effacer / détruire m , n , c
 - ▶ Garder S secret and publier P et x
 - ▶ m , n , c , S ne peuvent pas être (facilement)
dérivés de P et x car la factorisation de x est considérée
comme difficile (> 1200 chiffres)
mais ce n'est pas prouvé !
 - ▶ Ciphertext = $(\text{cleartext})^P \text{ mod } x$
 - ▶ Cleartext = $(\text{ciphertext})^S \text{ mod } x$
 $= (\text{cleartext})^{SP} \text{ mod } x$
 $= (\text{cleartext})^{kc+1} \text{ mod } x$
 $= (\text{cleartext})^{k(m-1)(n-1)} \text{ cleartext mod } x$
 $= \text{cleartext mod } x$
 $= \text{cleartext}$
- car en vertu du théorème d'Euler-Fermat
- $$z^{n-1} \text{ mod } n = 1 \text{ si } n \text{ est premier}$$
- (l'utiliser 2 fois : avec n et avec m)

Exemple – Le principe de RSA

► Petit exemple :

$$m=5 \quad n=11$$

$$x=55 \quad c=40$$

$$P=3$$

$$S=27$$

► Cleartext = 2

► Ciphertext = $(2)^3 \bmod 55 = 8$

► Cleartext = $(8)^{27} \bmod 55$

$$= 8^{20} \times 8^7 \bmod 55$$

$$= 8^4 \times 8^3 \bmod 55 \quad (\text{car } 8^{20} = 1 \bmod 55)$$

$$= 26 \times 17 \bmod 55$$

$$= 2 \bmod 55$$

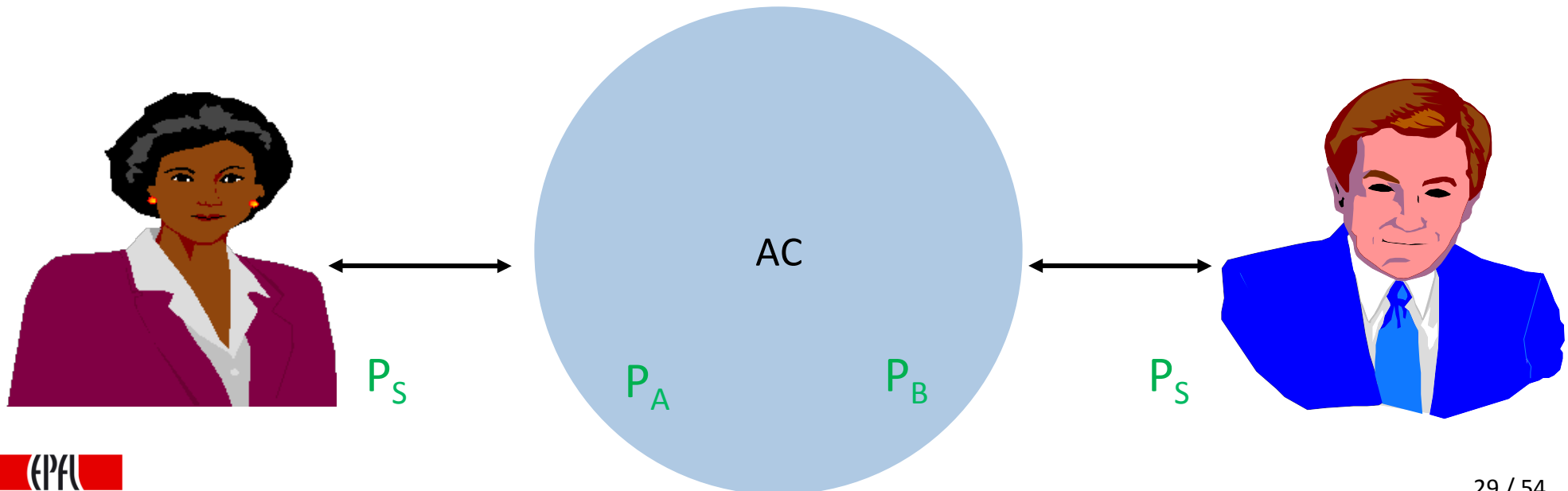
[Bien sûr $m=5$ et $n=11$ sont faciles à deviner étant donné $x=55$ parce que nous sommes tous capables de deviner les facteurs premiers de petits entiers comme x mais c'est pratiquement impossible pour des nombres de > 600 chiffres décimaux, même pour un ordinateur puissant car il n'y a pas d'algorithme efficace connu et une recherche exhaustive prendrait des siècles]

Comment savoir qu'on a la propre clé publique?

- ▶ Et non pas la clé d'un fraudeur?
- ▶ Ça s'appelle une attaque "phishing"
- ▶ Une "autorité de certification" distribue les clés publiques

Autorités de Certification des clés (AC)

- Communiquer avec un tiers implique de **connaître sa clé**
- Obtenir cette clé **face-à-face** est une rare possibilité quand Alice et Bob sont séparés par un réseau
- Echanger ces clés **via le réseau** n'est pas sécurisé – elles pourraient être falsifiées par un intrus ...
- ... à moins d'être **enveloppées dans un certificat** = message signé par une autorité de confiance
- C'est ce que sont les ACs – **des tiers de confiance** se portent garants de clés publiques authentiques
- Plusieurs ACs peuvent **mutuellement certifier leurs clés publiques**
pour assurer l'authenticité des clés publiques de tiers certifiés par différents ACs



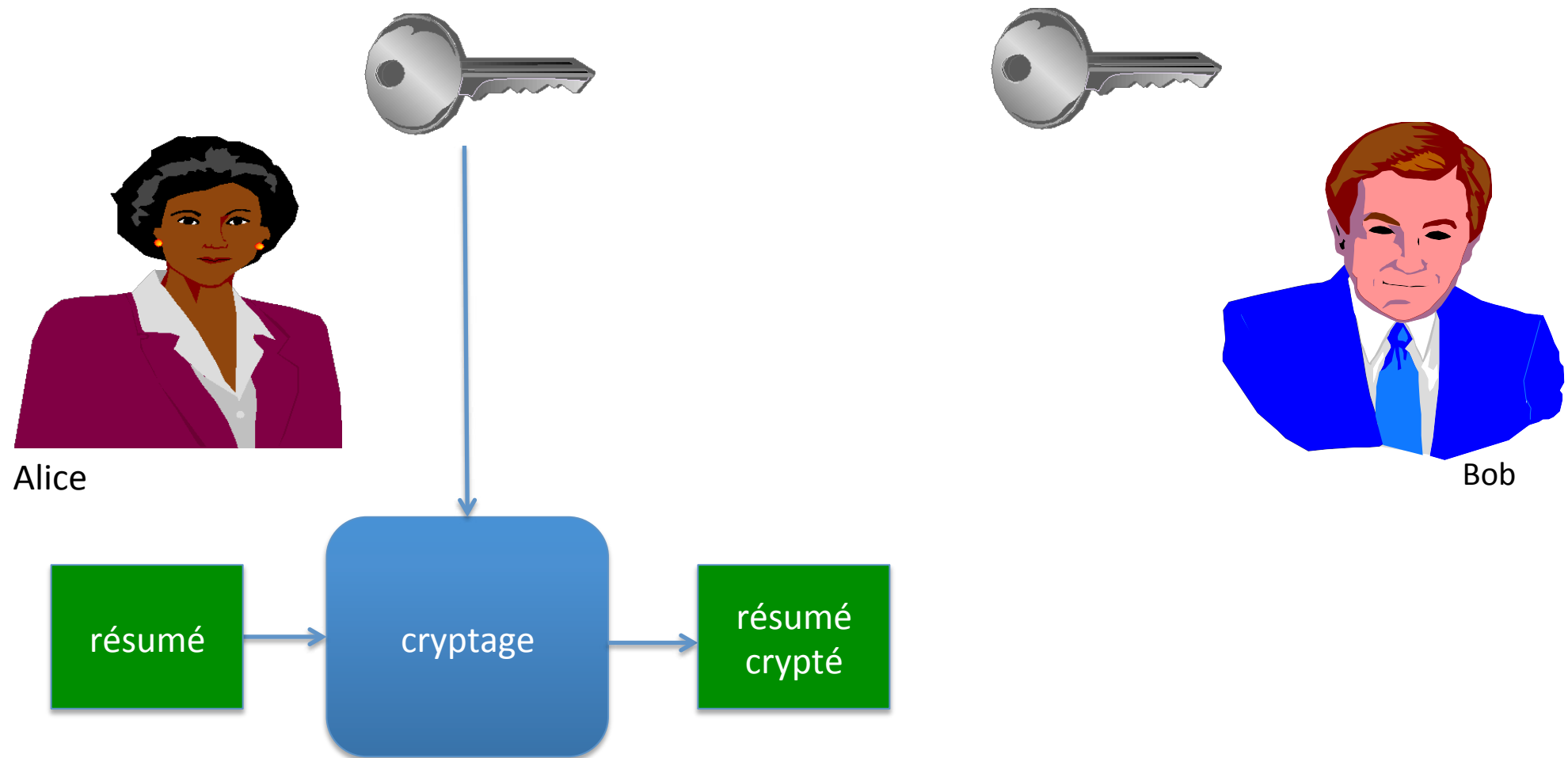
Intégrité: Menace / Défense

- ▶ Menace: modifications des données
- ▶ Défense: la cryptographie

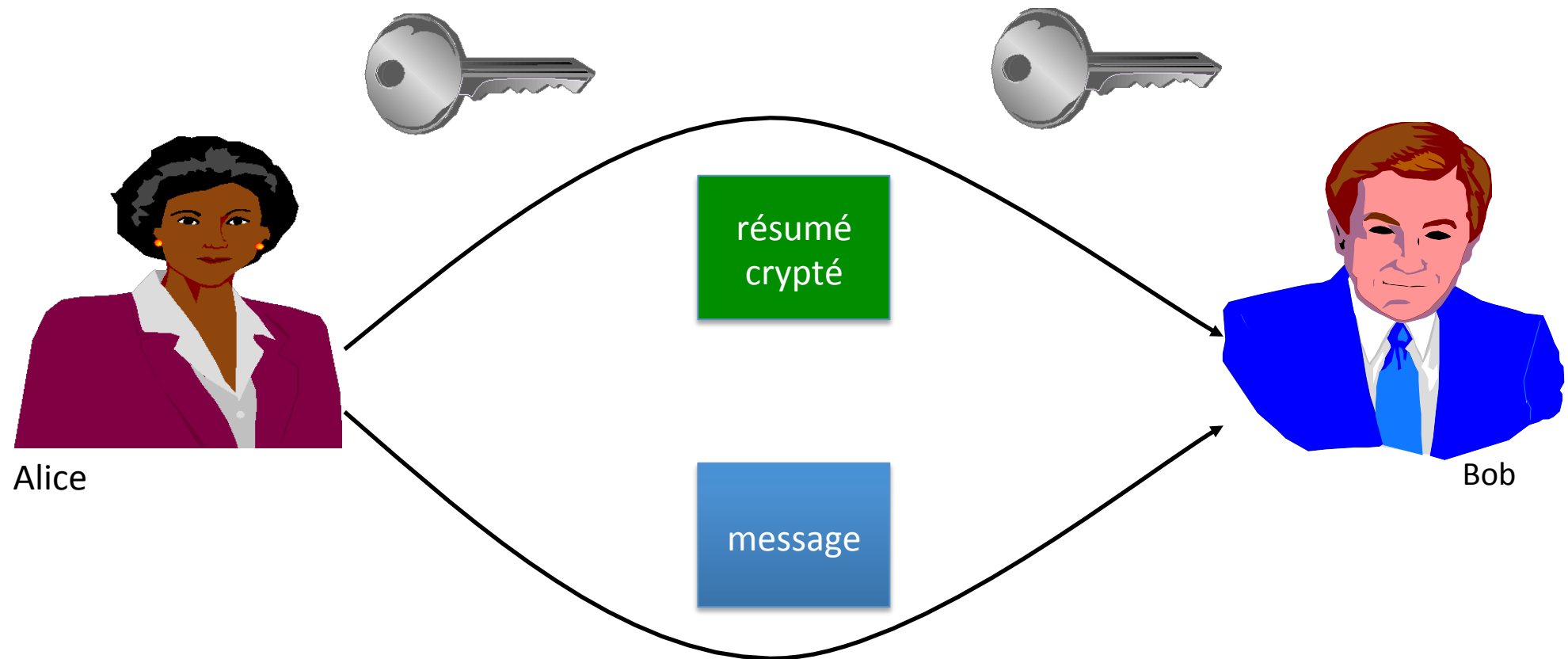
Intégrité à base de cryptographie symétrique



Intégrité à base de cryptographie symétrique



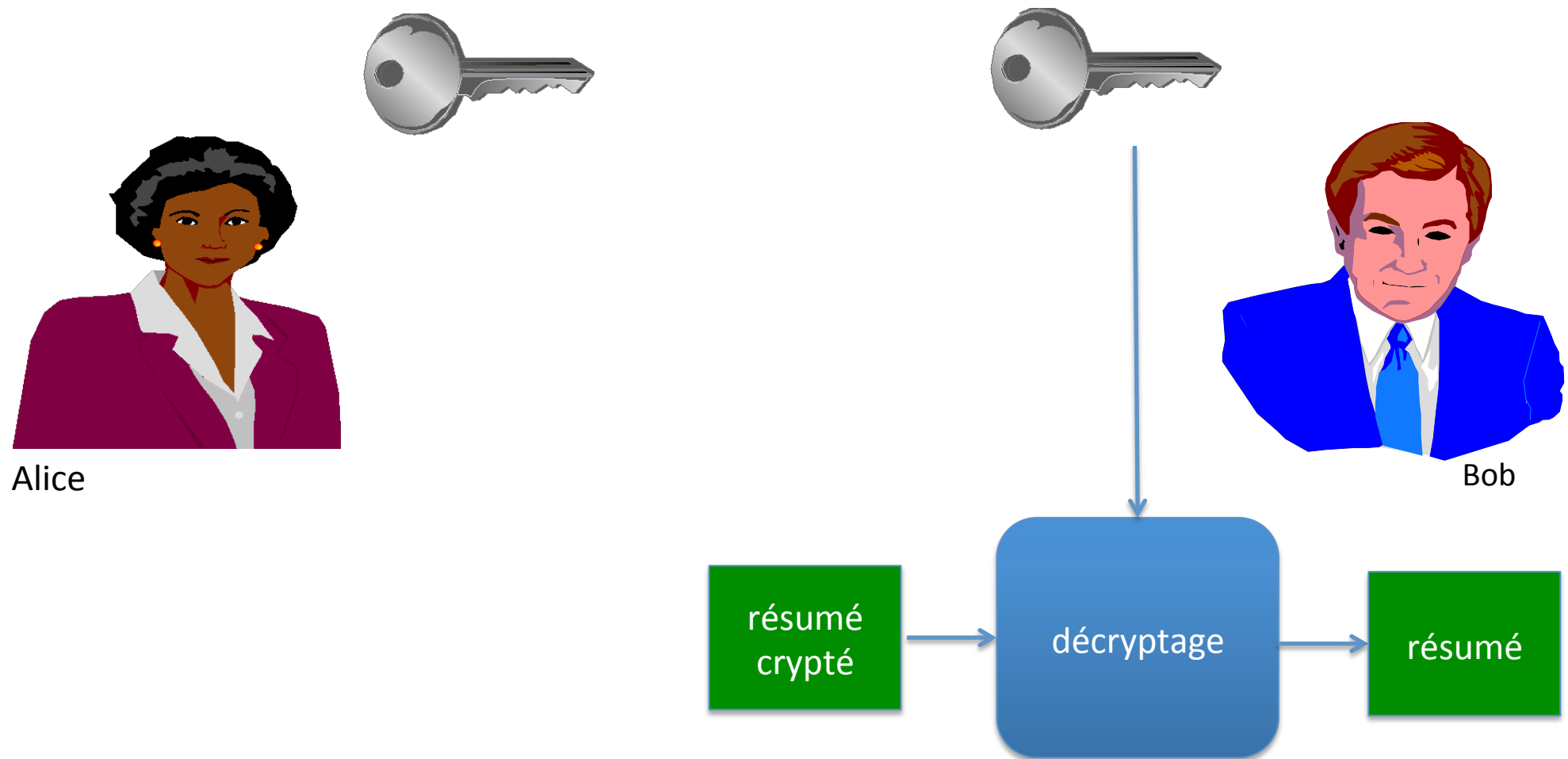
Intégrité à base de cryptographie symétrique



Intégrité à base de cryptographie symétrique



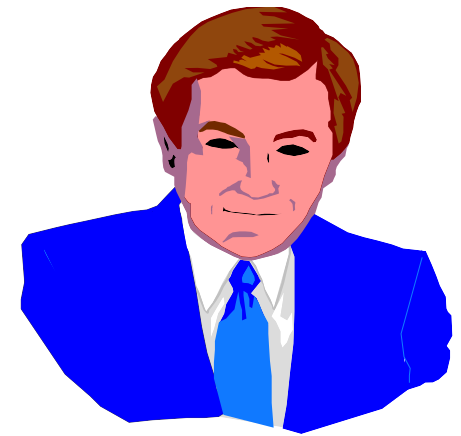
Intégrité à base de cryptographie symétrique



Intégrité à base de cryptographie symétrique



Alice



Bob

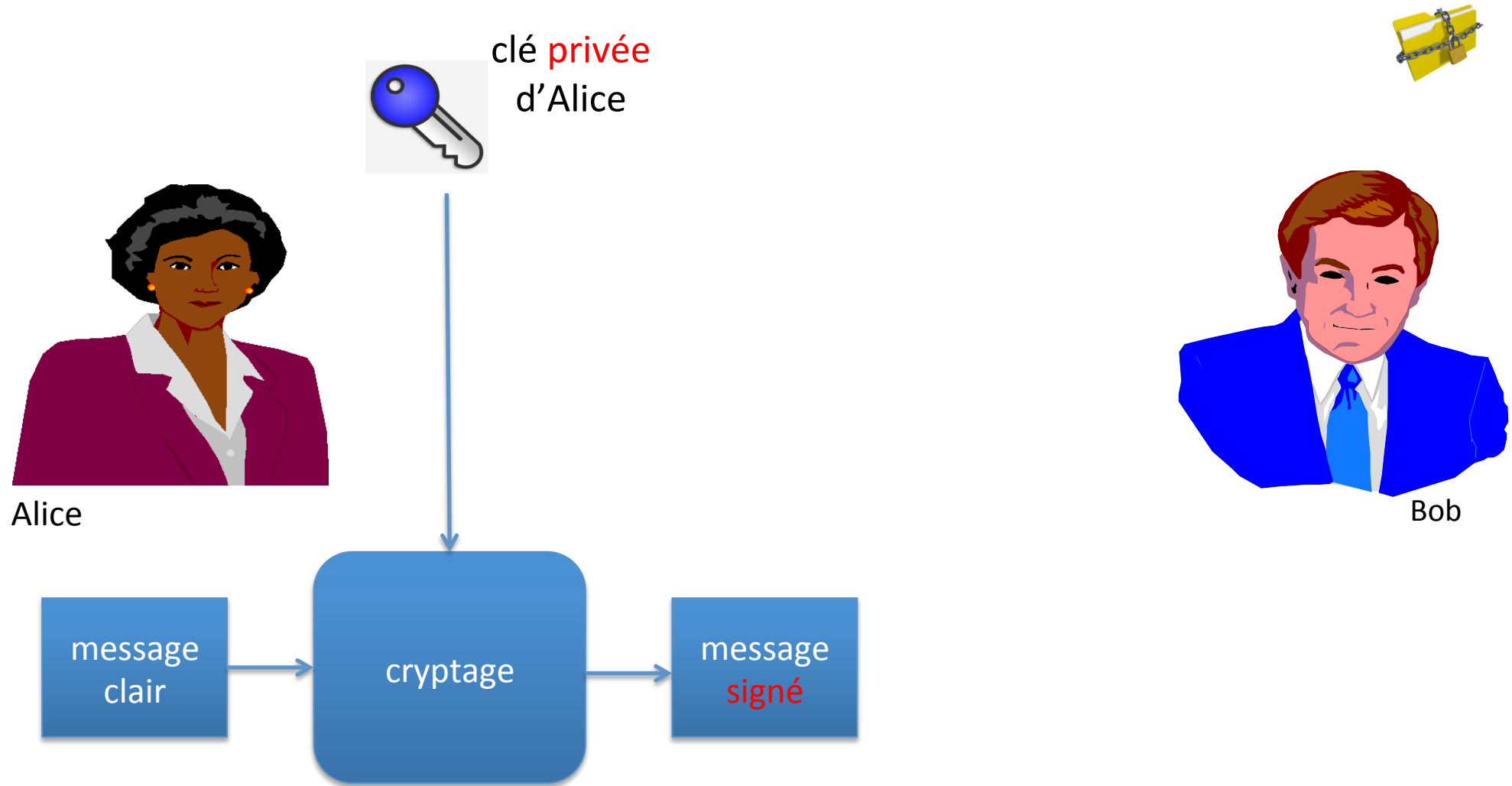
Résumé calculé par Bob \neq Résumé envoyé par Alice

→ Le message a été altéré pendant sa transmission

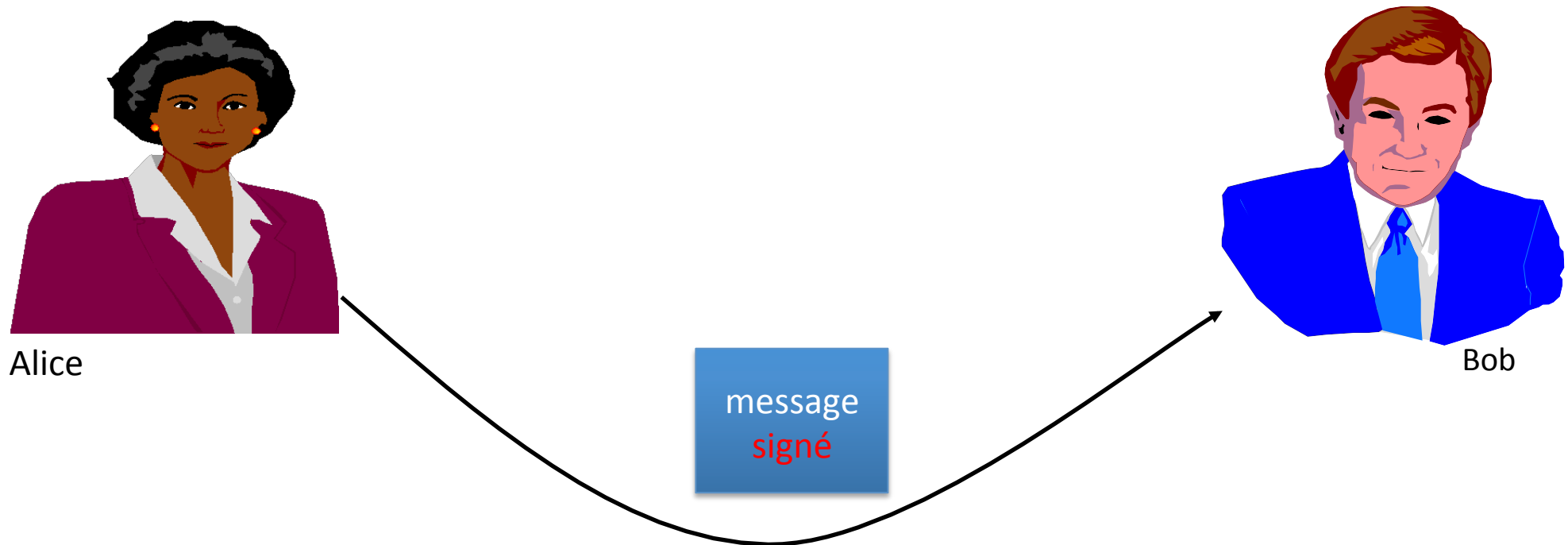
Responsabilité: Menace / Défense

- ▶ Menace: le démenti
- ▶ Défense: la signature digitale par la cryptographie asymétrique

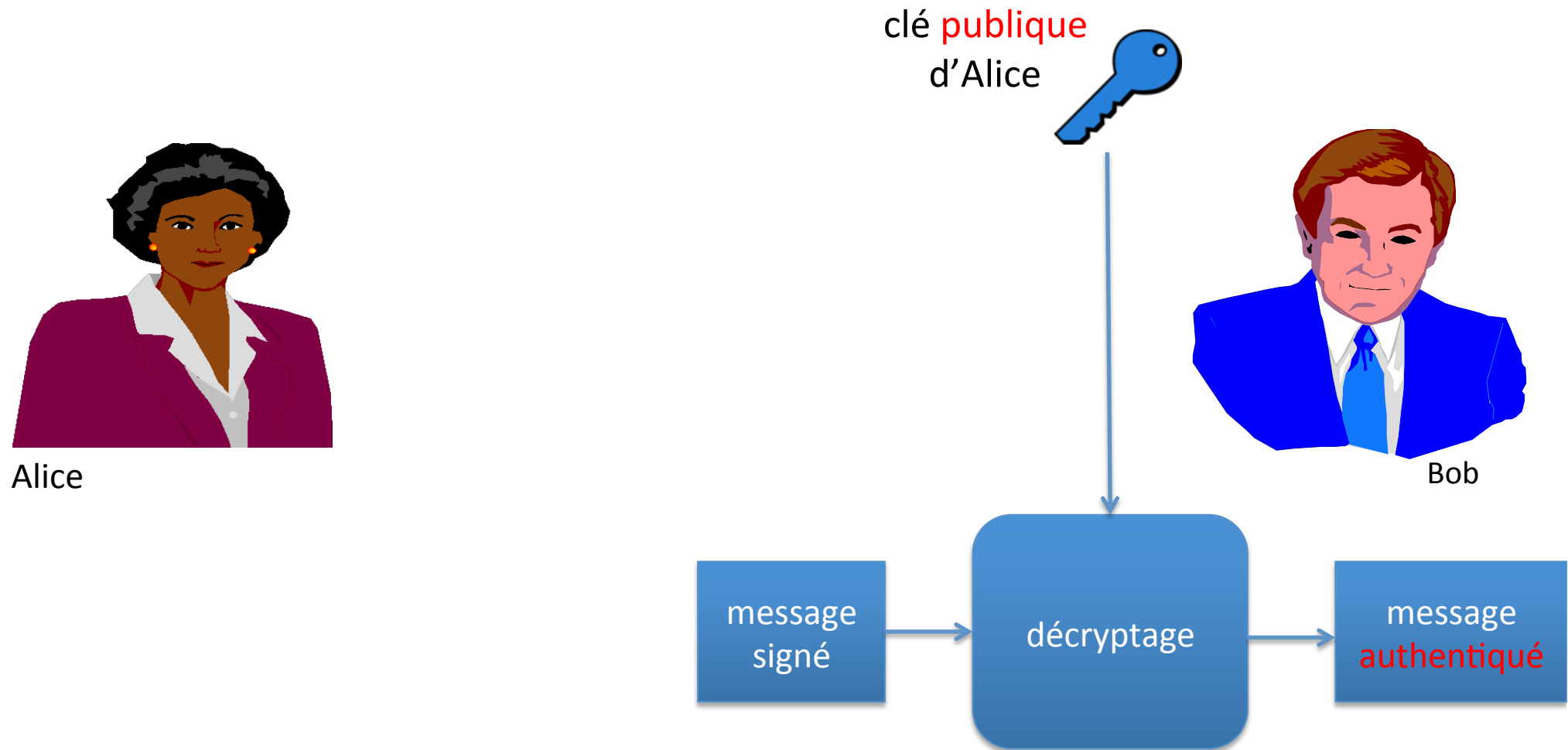
La cryptographie asymétrique



La cryptographie asymétrique

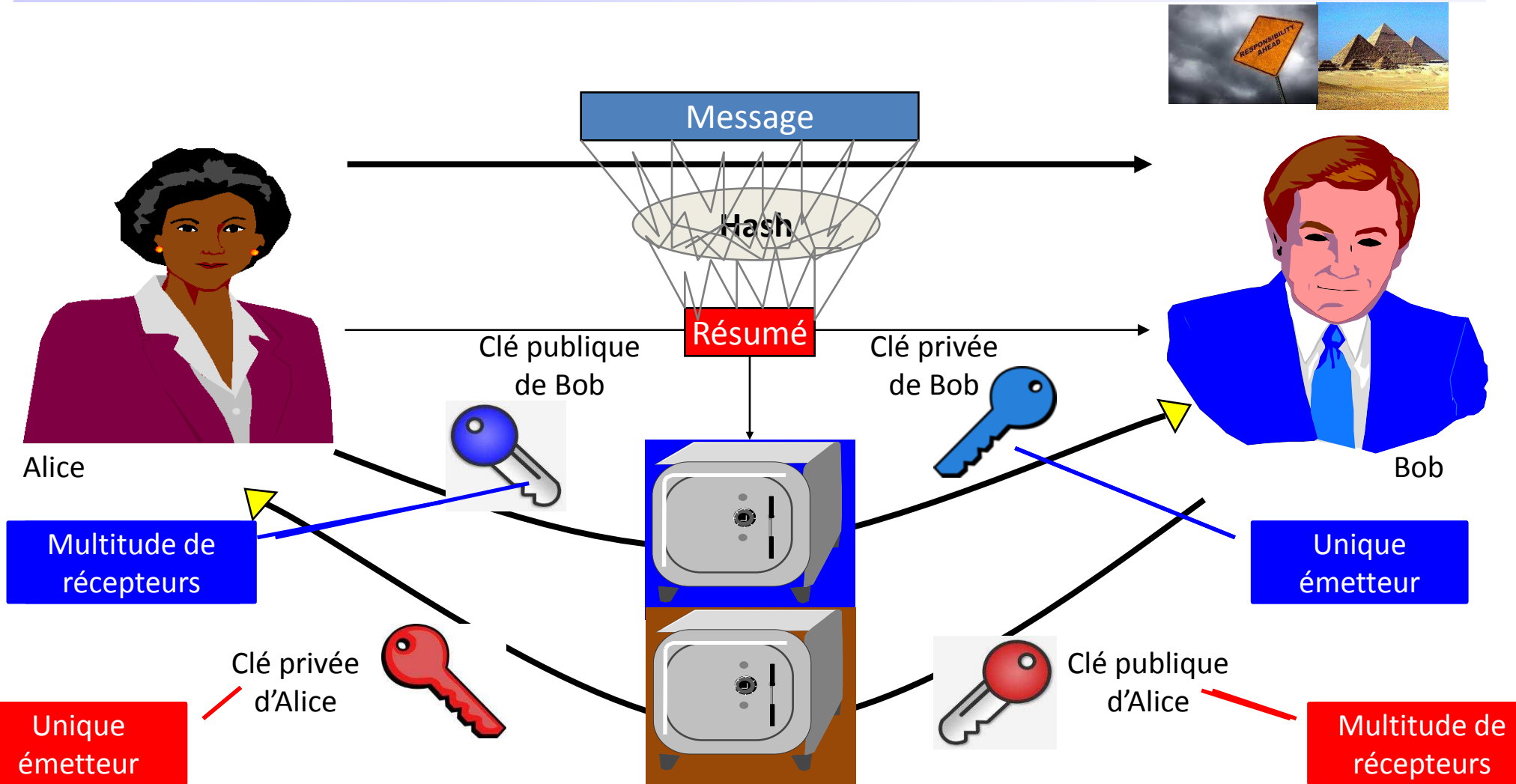


La cryptographie asymétrique



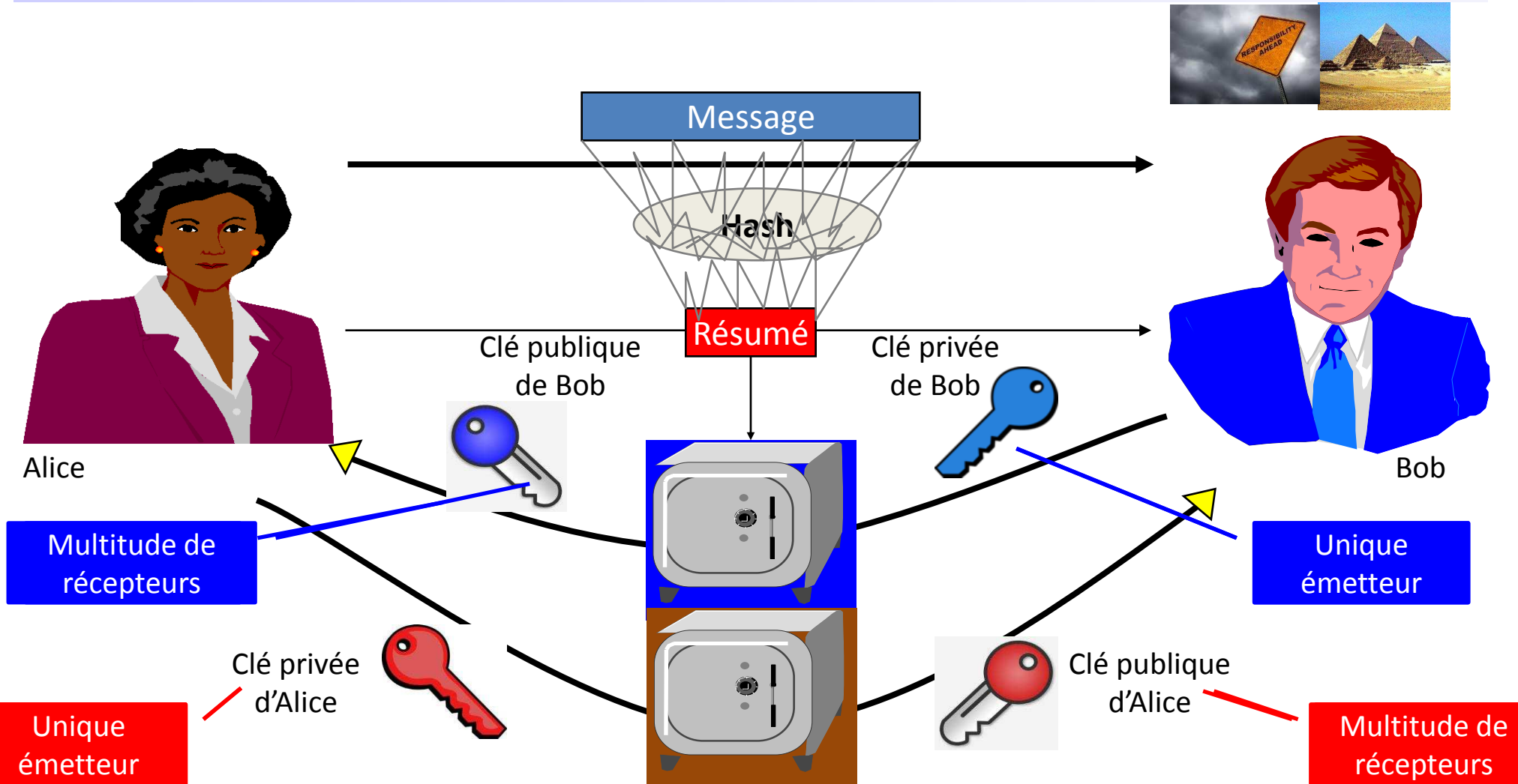
Intégrité ET signature digitale => authenticité / responsabilité

Cas asymétrique – Exemple en réseau



Intégrité ET signature digitale => authenticité / responsabilité

Cas asymétrique – Exemple en réseau



Plan de la leçon

- ▶ Principes de base
- ▶ Confidentialité, intégrité et responsabilité : cryptographie
- ▶ **Authentification**
 - ▶ Nos identités : Sécurisation de la sphère privée
 - ▶ Authentification
 - ▶ par ce que l'on connaît
 - ▶ par ce que l'on est
 - ▶ par ce que l'on détient
 - ▶ Gestion (électronique) de nos identités
- ▶ Autorisation
- ▶ Règles de bonne conduite
- ▶ Résumé / Vue d'ensemble

Usurpation d'identité: Menace / Défense

- ▶ Menace: l'usurpation d'identité
- ▶ Défense: l'authentification

Sécurisation de la sphère privée

► Définition

► Limites

► Menaces

► Défenses

“In the world of Big Data
privacy invasion is the
business model ! ”

(CNET headline news 2012-02-29)

Le fond de commerce des réseaux sociaux est notre sphère privée

Sphère privée – Définition

► Nous avons tous une identité à plusieurs facettes

▪ Comme

- Citoyen
- Consommateur
- Employé ou indépendant
- Patient
- etc.

• Notez le lien:

Identité => sphère privée => réputation

▪ Toutes les facettes de notre identité ne sont pas nécessairement publiques

- Le **vote** d'un citoyen doit pouvoir rester secret
- L'**opinion** d'un consommateur doit pouvoir rester anonyme
- Des collègues de travail peuvent avoir une **liaison** discrète tout à fait honorable
- Quelqu'un doit pouvoir acheter un **médicament** sans être suspecté de maladie

► La protection de la sphère privée consiste à garder ces facettes isolées les unes des autres

► La protection de la sphère privée ne consiste PAS à cacher des activités illégales / immorales

► La plupart des gens ne se soucient de leur sphère privée ... **que quand ils l'ont perdue**

► L'enjeu est l'intégrité de leur réputation



Sphère privée – Limites

- ▶ La protection de la sphère privée est un **droit fondamental**
- ▶ Mais la société a besoin de responsabilité pour **trouver et punir activités illégales / immorales**

Où est la limite entre surveillance et espionnage?

- ⇒ Pas de réponse absolue et donc pas de réponse dans ce cours
- ⇒ Chaque société doit décider pour elle-même où sont les limites
 - Utiliser un GPS pour localiser un véhicule volé peut être légitime
Utiliser le même GPS pour faire suivre son chauffeur est abusif
 - Déposer une plainte anonyme contre un employeur abusif peut être légitime
Colporter un ragot anonyme qui peut nuire à un tiers est abusif

Sphère privée – Menaces

<http://www.youtube.com/embed/F7pYHN9iC9I?rel=0>

- ▶ De plus en plus de données (privées) sont **récoltées** électroniquement
 - Les communications Internet ne sont plus protégées comme des lignes téléphoniques
Toutes peuvent identifier des individus ou même des groupes
 - Entreprises et gouvernements profitent de ce vide juridique
- ▶ De plus en plus de données (privées) sont **stockées** électroniquement
 - En des lieux et sous des juridictions que le “cloud” rend toujours plus flous (v. Leçon 12)
- ▶ De plus en plus de données (privées) sont **échangées** électroniquement
 - Des entreprises commerciales vivent de la revente de ces données privées
- ▶ De plus en plus de données (privées) sont **analysées** électroniquement
 - Des entreprises sont spécialisées dans la corrélation de données isolées
- ▶ De plus en plus de données (privées) sont **publiées** électroniquement
 - pastebin.com est un bazar de publication de données confidentielles
- ▶ De plus en plus la sphère privée d'un individu est **maintenue** par des tiers
 - Elle échappe aux intéressés eux-mêmes (v. plus loin la gestion d'identités)
- ▶ Obtenir assez de données privées pour **usurper une identité** est devenu relativement simple



Sphère privée – Principes de protection



► Au-delà de l'accès, la protection de la sphère privée concerne l'usage des informations

► Au-delà des contrôles d'accès, le contrôle de l'usage requiert une politique stipulant:

- Quelles informations sont collectées
- Comment les informations sont sécurisées
- Combien de temps elles sont gardées (avant d'être effacées)
- A quelle fin elles peuvent être utilisées
- A qui elles peuvent être transmises

Nous ignorons les conséquences possibles de la vie dans un monde qui n'oublie plus jamais rien !!

► Ces politiques doivent aussi garantir un contrôle aux individus concernés

- Aucune collection par défaut avec une possibilité de l'autoriser (= "opt-in") plutôt qu'une collection par défaut avec une possibilité de l'interdire (= "opt-out")
- Ils doivent avoir un droit d'inspecter ce qui est collecté
- Ils doivent avoir un droit de corriger ce qui est collecté
- Ils doivent être informés en cas de violation
- Ils doivent avoir un droit d'appel en cas de litige

► De telles politiques sont typiquement confuses et non-intuitives pour le commun des mortels

Authentification à distance

► Trois possibilités sur base de

- Quelque chose que l'utilisateur **connaît**: NIPs et mots de passe
- Quelque chose que l'utilisateur **est**: biométrie
- Quelque chose que l'utilisateur **détient**: jetons



Authentification sur base de quelque chose que l'utilisateur connaît: Userid et mot de passe ou NIP

- ▶ Les **userids** devraient être aussi difficiles à deviner que les mots de passe pour protéger les identités
- ▶ Les mots de passe doivent être **stockés** sur l'ordinateur qui les vérifie
=> Ils sont exposés => Il ne faut pas les stocker en texte clair
- ▶ Les mots de passe doivent être **transmis** à l'ordinateur qui les vérifie
=> Ils sont exposés => Il ne faut pas les transmettre en texte clair
- ▶ Les mots de passe doivent être **rentrés** dans le terminal qui les capture
=> Ils sont exposés au "shoulder surfing"
 - Il faut **supprimer leur affichage** à l'écran
 - Il faut **cacher leur saisie** au clavier
 - Il faut s'assurer **qu'aucune caméra** ne surveille le clavier
 - Il faut s'assurer **qu'aucun maliciel** n'espionne le clavier (key-logger – risque majeur)
ou n'enregistre les émanations électromagnétiques
- ▶ Les mots de passe ne doivent **JAMAIS** être écrits nulle part
=> Ils doivent être **facile à mémoriser** – mais **difficile à deviner**



Les 500 mots de passe les plus stupides en 2008

Source: <http://www.whatsmypass.com/?p=415>

123456

290'731 instances sur 32M
de mots de passe analysés!

l'immatriculation du Starship
Enterprise dans la série Startrek

les 6 premières touches de
gauche sur un clavier qwerty

le titre du 1er film
de George Lucas

ncc1701

thx1138

un no. de tél.
mentionné
dans une
chanson de
Tommy
Tutone en
1982

le titre d'un album de Van Halen en 1988

qazwsx

8675309

ou812

Les 500 mots de passe les plus stupides en 2008

- ncc1701 = l'immatriculation du Starship Enterprise dans la série Startrek
- thx1138 = le titre du 1er film de George Lucas
- qazwsx = les 6 premières touches de gauche sur un clavier qwerty
- ou812 = le titre d'un album de Van Halen en 1988
- 8675309 = un numéro mentionné dans une chanson de Tommy Tutone en 1982 qui a causé une "épidémie" d'appels à Jenny au poste 867 53 09

- Près de 50% des gens utilisent des noms, de l'argot ou des mots de passe triviaux (touches de clavier, lettres, ou chiffres consécutifs, etc.)

Environ 10% des gens utilisent au moins un mot de passe de la liste précédente

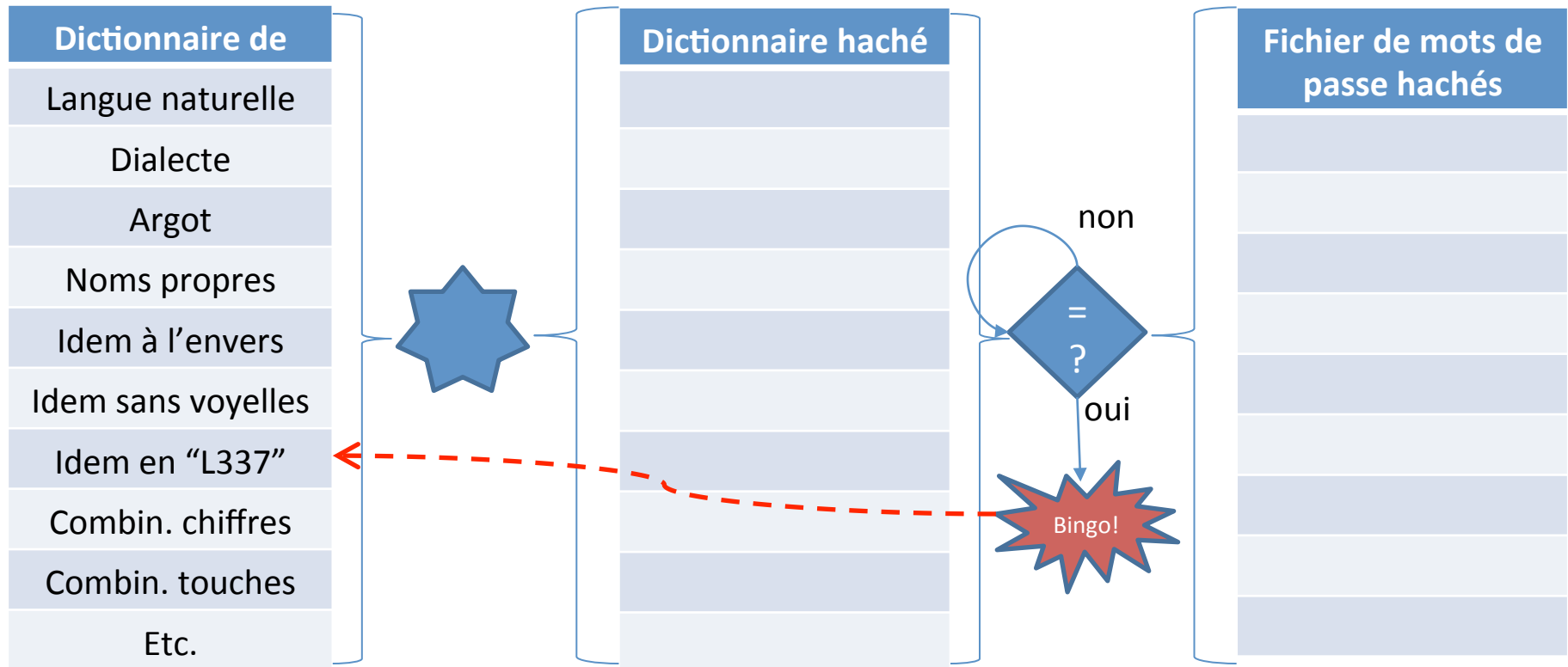
Et 2% des gens utilisent un des 20 premiers mots de passe de cette liste

- Les utilisateurs sont si prévisiblement stupides que les pirates utilisent précisément ces trucs, pour tenter de pénétrer les ordinateurs en se faisant passer pour leurs victimes
C'est ce qu'on appelle les **attaques au dictionnaire** de mots de passe

Une attaque au dictionnaire

- ▶ L'attaquant traverse le dictionnaire
- ▶ Fait des simples substitutions
 - Majuscule – minuscule
 - Lettre – chiffre
 - Etc.
- ▶ Ou essaie carrément toutes les combinaisons possibles

Attaques de mots de passe au dictionnaire



- Le “salage” est nécessaire mais pas suffisant contre ces attaques au dictionnaire
10% des mots de passe salés + hachés ont été cassés en 4 heures, 53 minutes, et 6 secondes!
 parmi la liste de 860'160 mots de passe exposée par l'attaque de Strategic Forecasting en 2011
<http://www.thetechherald.com/articles/Report-Analysis-of-the-Stratfor-Password-List>)

Comment choisir des mots de passe

- ▶ Une longueur suffisante
- ▶ Utiliser des alphabets assez vastes
 - Majuscules + minuscules + chiffres (62)
 - Caractères spéciaux, mais pas toujours acceptés
- ▶ Changer de mot de passe régulièrement

Comment choisir un mot de passe

- Les mots de passe doivent avoir une longueur suffisante pour résister aux devinettes
 Risque $R = \text{durée de vie } D \times \text{fréquence des attaques } F / \text{taille de l'alphabet } T^M$ (taille du mot de passe)

$$M > \log \left(\frac{D \times F}{R} \right) / \log T$$

$$8 > \log \left(\frac{100 \text{ J} \times 100 / \text{J}}{10^{-9}} \right) / \log 62$$
- => **Utiliser des alphabets assez vastes** – majuscules + minuscules + chiffres (62)
 Des caractères spéciaux seraient bien mais pas acceptés par tous les systèmes
- => **Limiter la fréquence des attaques** pour déjouer des attaques programmées systématiques
 Terminer toute connection après quelques échecs
- => **Changer de mot de passe régulièrement** (chaque année ou même chaque trimestre)
- => **Ne jamais réutiliser le même mot de passe** sur plusieurs systèmes (“password sloth”)
- Ne jamais choisir un mot de passe dans un **langage naturel ou un dialecte quelconque**
 - Ne pas remplacer des lettres par des chiffres évidents
 - e.g. 0 for O, 1 for I, 2 for Z, 3 for E, 4 for A, 5 for S, 6 for G, 7 for T, 8 for B, 9 for q
 - Ne pas épeler à l'envers, éliminer les voyelles, employer lettres pour phonèmes, etc.
 Si cela paraît malin, les auteurs d'attaques au dictionnaire y ont aussi déjà pensé !
- **Testez vos mots de passe avec des outils de confiance qui travaillent en mode crypté**
 p.ex. <http://ophcrack.sourceforge.net/> (EPFL)

Alternatives et compléments aux mots de passe **(aussi à graver en mémoire mais jamais sur papier / en machine)**

- ▶ **Phrases** de passe – entropie plus grande au prix de plus de caractères
- ▶ **Questions** de passe – répondre à des questions personnelles subtilement choisies
- ▶ **Graphes** de passe – cliquer en séquence sur des images positionnées aléatoirement
- ▶ **Algorithmes** de passe – construire les mots de passe selon un algorithme simple mais secret

phrase fixe
(p.ex. dans une langue étrangère)

descripteur
du système

descripteur
de l'année

w	t	i	h	T	A	2	m
a	o	w	i	H	D	m	m
s	s	a	d	I	W	i	x
a	u	o	e	N	5	I	i
b	s	i	s	K	1	1	i
i	h	s	u	P	0	3	i

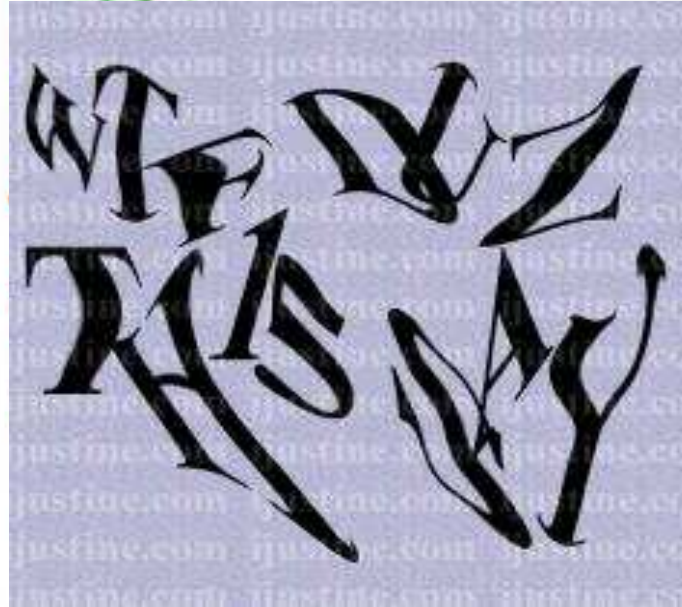
Autres risques

- ▶ Le stockage (jamais en texte clair)
- ▶ La transmission (jamais en texte clair)
- ▶ La rentrée dans le terminal
 - Supprimer leur affichage à l'écran
 - Cacher la saisie au clavier
 - S'assurer qu'aucune caméra ne surveille le clavier
 - S'assurer qu'aucun maliciel n'espionne le clavier

Puzzles de passe et CAPTCHAs

“Completely Automated Public Turing Test to Tell Computers and Humans Apart”

- N'authentifie pas un utilisateur mais prouve qu'il n'est pas une machine et empêche ainsi des attaques ou tentatives de transactions programmées
- Sur base de puzzle, tel que reconnaître une séquence de lettres déformées
Généralement efficace mais la reconnaissance automatique de CAPTCHAs progresse (ou peut faire l'objet de crowdsourcing)

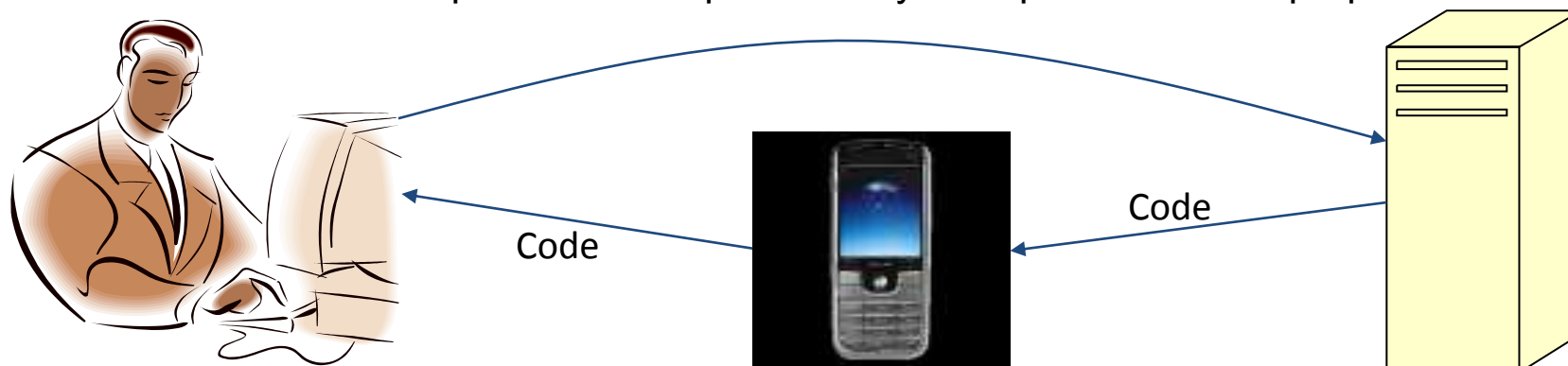


Authentification à deux canaux et deux facteurs

► Quand les mots de passe ne sont plus assez sûrs pour une application critique ...

► ... on a recours à une authentification à double canal

- L'ordinateur envoie un code aléatoire à l'utilisateur par un canal secondaire
 - e.g. SMS comme le font par exemple Google ou Swisscom Wi-Fi
- L'utilisateur rentre le code dans son ordinateur
 - Alternativement le téléphone mobile peut renvoyer un portrait de son propriétaire



NB: des criminels de haut vol ont déjà surmonté une telle authentification

► ... ou on a recours à une authentification à double facteur

- Biométrie ou jeton d'identification en plus du mot de passe

Authentification sur base de quelque chose qu'un utilisateur **est**: Biométrie

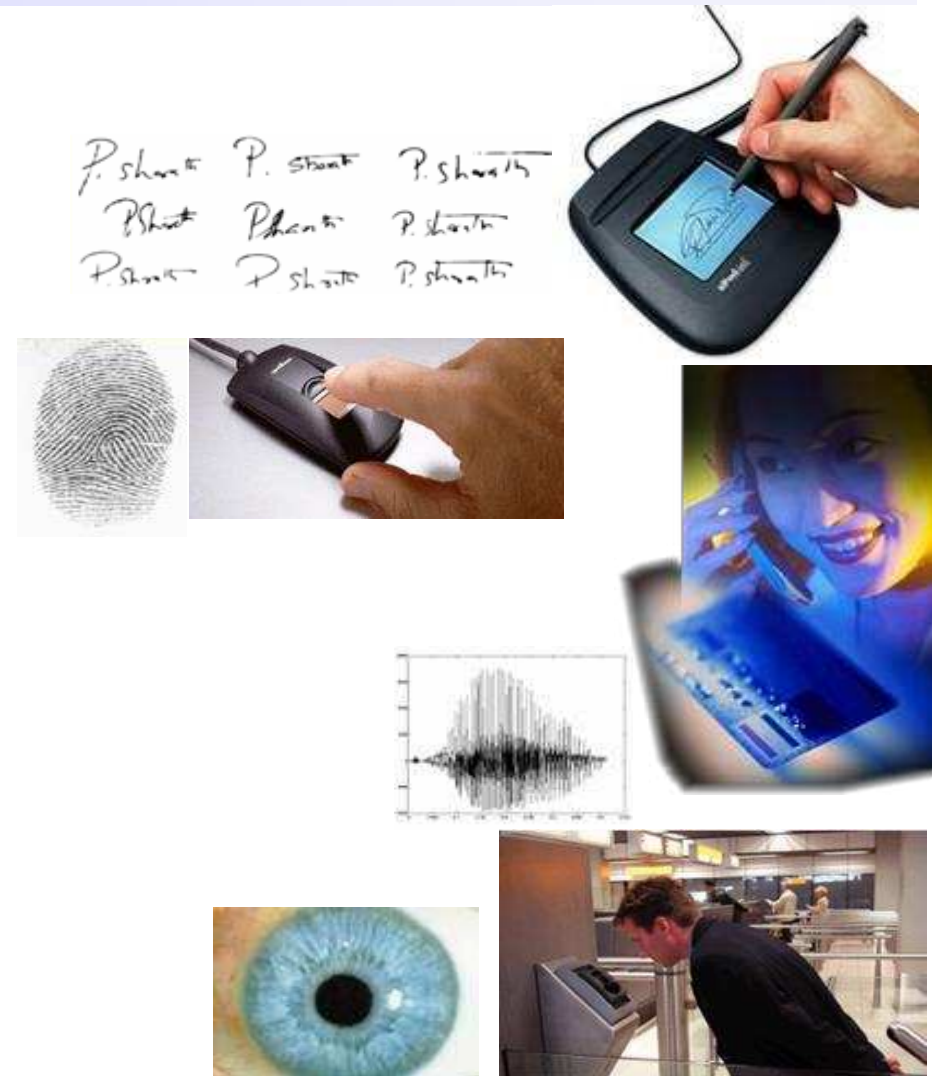
- ▶ La biométrie est en fait la méthode **d'authentification originelle** de l'humanité
 - Ce qui est neuf est son **utilisation en informatique**

- ▶ La biométrie d'un individu est **unique mais pas secrète**
 - Le **vol** d'identité biométrique est donc un risque majeur
(<http://www.youtube.com/watch?v=3M8D4wWYgsc>)

- ▶ La vérification biométrique est encline à erreurs
 - Des **faux négatifs** sont ennuyeux
 - Des **faux positifs** sont indésirablesTrouver un compromis entre les deux est délicat
=> La biométrie est souvent utilisée comme **second facteur** plutôt que comme seul facteur

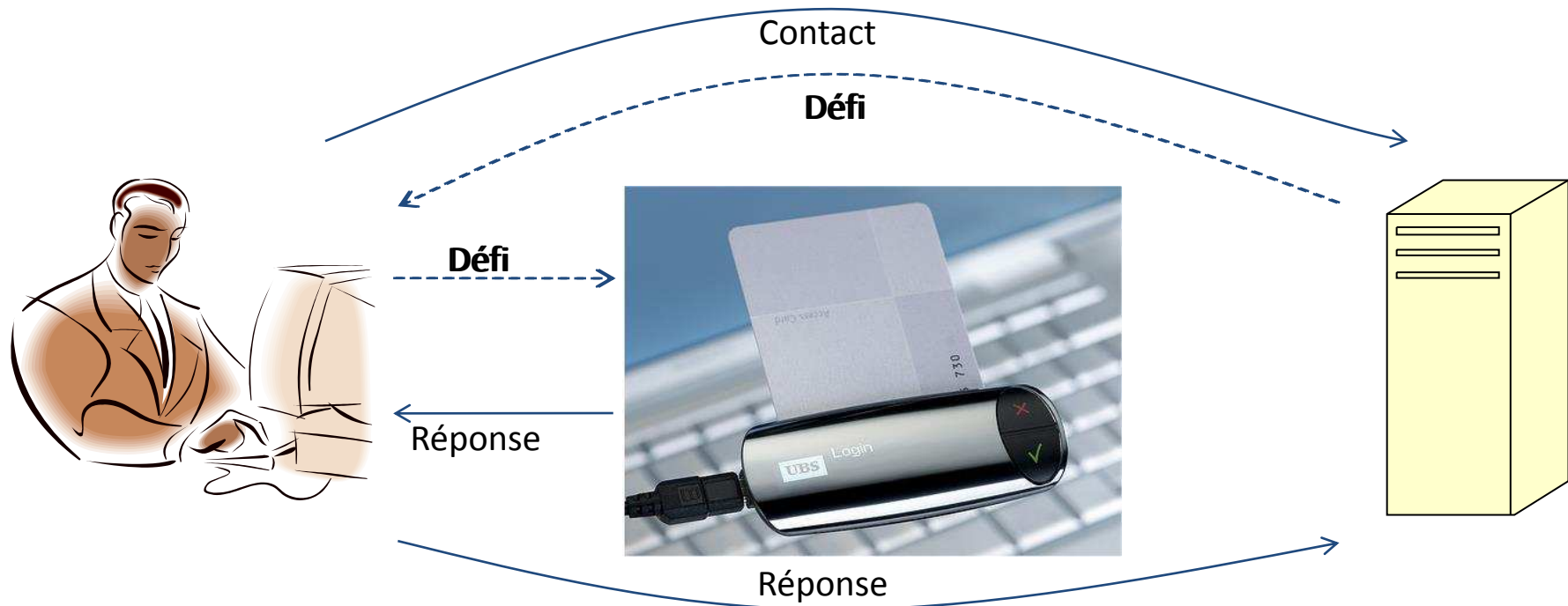
Techniques biométriques

- ▶ Profil et vitesse de **dactylographie**
 - Peu précis
- ▶ Reconnaissance dynamique de **signature**
 - Sûr mais cher
- ▶ Reconnaissance des **veines** de la paume de main
 - Sûr mais cher et peu pratique
- ▶ Reconnaissance de la **forme** de la main
 - Sûr mais cher et peu pratique
- ▶ Reconnaissance des **empreintes** digitales
 - Commune mais peu sûre (à moins d'exiger un poulx)
- ▶ Reconnaissance de la **voix**
 - Ni très sûr ni très consistant (faux négatif)
- ▶ Reconnaissance du **visage**
 - Ni très sûr (photo) ni très consistant (vieillesse)
- ▶ Reconnaissance de **l'iris** de l'oeil
 - Pas très sûr à moins d'exiger un oeil "vivant"
- ▶ Reconnaissance de **l'ADN**
 - Parfait ... pour la science fiction




Authentification sur base de quelque chose qu'un utilisateur **détient**: Jeton USB avec ou sans interface machine et interface utilisateur

- Basé sur un échange de codes ou un envoi de cachet-dateur chiffrés



- Avec un tel jeton non seulement l'utilisateur mais **chaque transaction peut être identifiée**
- **Un maliciel ne peut pas interférer** car l'utilisateur confirme chaque transaction sur le jeton

Authentification bi-directionnelle

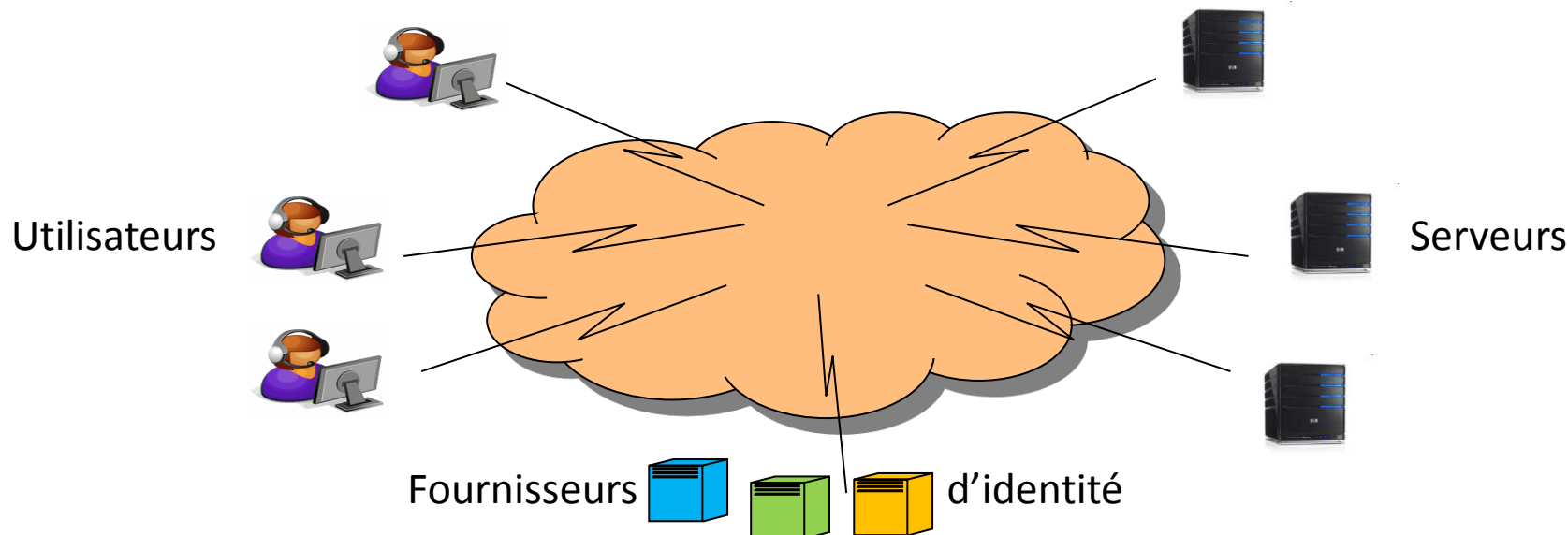
- ▶ Toutes les techniques vues jusqu'ici n'offrent qu'une authentification **UNIDIRECTIONNELLE**
- ▶ Ceci représente une carence et un risque **MAJEUR** ("phishing / pharming")
 - Un service frauduleux peut se présenter sous l'identité d'un service réputé et ainsi récolter les identités et mots de passe d'utilisateurs innocents et crédules
- ▶ Le problème est que sans cryptographie,
 - le premier partenaire qui s'identifie à l'autre doit lui révéler son identité et son mot de passe
- ▶ La solution est une identification **bi-directionnelle**
 - Cryptographique de la part de l'ordinateur (sur base de défi ou de cachet-dateur crypté)
 - Cryptographique ou non de la part de l'utilisateur
 - Le cas cryptographique requiert un jeton avec interface machine
 - C'est exactement ainsi que fonctionnent les protocoles HTTPS / SSL / TLS
 - Ce qui est indiqué par la présence de l'icône  dans une des barres du navigateur

Plan de la leçon

- ▶ Principes de base
- ▶ Confidentialité, intégrité et responsabilité : cryptographie
- ▶ Authentification
 - ▶ Nos identités : Sécurisation de la sphère privée
 - ▶ Authentification
 - ▶ **Gestion (électronique) de nos identités**
- ▶ Autorisation
- ▶ Règles de bonne conduite
- ▶ Résumé / Vue d'ensemble

Gestion de l'identité

- ▶ Pour pouvoir authentifier un utilisateur il faut
 - Le **définir** au système = lui attribuer une **identité** vérifiable
 - L'**enregistrer** dans le système et lui attribuer le mot de passe ou jeton nécessaire
 - Le "**dé-registrer**" du système et invalider ses attributs quand il quitte l'organisation
- ▶ **N utilisateurs x M serveurs font de ces processus un véritable cauchemar de complexité**
 - Redéfinition du même utilisateur dans M serveurs
 - Avalanche de mots de passe pour chaque utilisateur
- ▶ **Solution => fournisseurs d'identité** (p.ex. OpenId)



Qu'est-ce qu'une identité?

<http://sixminutes.dlugan.com/presentation-20-hardt-executes-the-lessig-method/>

- “On the Internet anyone can be a dog”
... or a cat

p.ex. 666@hotmail.com ou geek@gmail.com
ou même les identifiants OpenId
sont des identités non-avérées



- Les serveurs garants d'identités **avérées suivent le modèle des cartes de crédit**

- Serveurs et utilisateurs peuvent **choisir** le garant d'identité à leur guise
- L'acceptation auprès du garant est cependant sujette à **vérification**
- La **responsabilité** du garant est engagée et garantit celle de l'individu
- De tels systèmes s'étendent bien à un monde **global**



- **Identités électronique et traditionnelle (administrative) se rejoignent d'ailleurs**

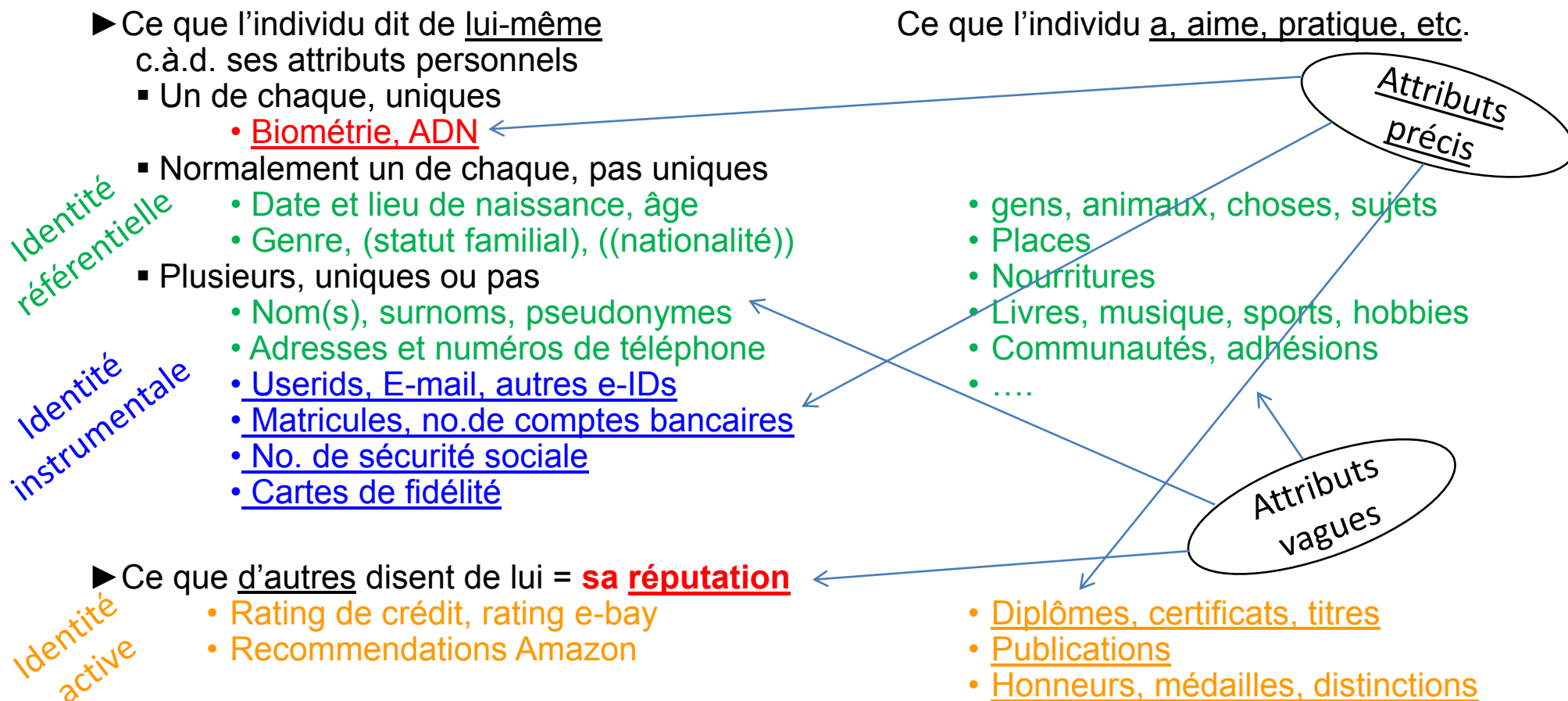
- Cartes bancaires, cartes de crédit, cartes SIM, etc. offrent déjà des identités avérées
- Cartes d'identité, passeports, permis de conduire deviennent électroniques par sureté

- La question est “qu'est-ce qui constitue une identité (électronique) **avérée**?”

Sécurité de l'Information	Sécurité des Communications	Sécurité du Calcul
Authentification	Identification	Sécurisation des réseaux

En quoi consiste l'identité d'un individu ?... Sa vie privée !!

Qui "détient" sa version électronique ?... Pas lui !!



=> Grande valeur et graves conséquences en cas de dommage



Sécurité de l'Information	Sécurité des Communications	Sécurité du Calcul
Authentification	Identification	Sécurisation des réseaux

L'identité d'un individu est relative et dynamique

- Elle est une façon **contextuelle** de faire référence à cet individu
 - L'individu concerné peut même en ignorer certaines facettes

フィル ヤンソン
フィル ジャンソン

פיליף ג'נסון

Фил Янсон

菲尔·詹森
詹森菲尔

فيل جانسن

फिल जानसन

- Elle **évolue** avec le temps
 - Les attributs qui la composent peuvent changer, devenir périmés ou invalides

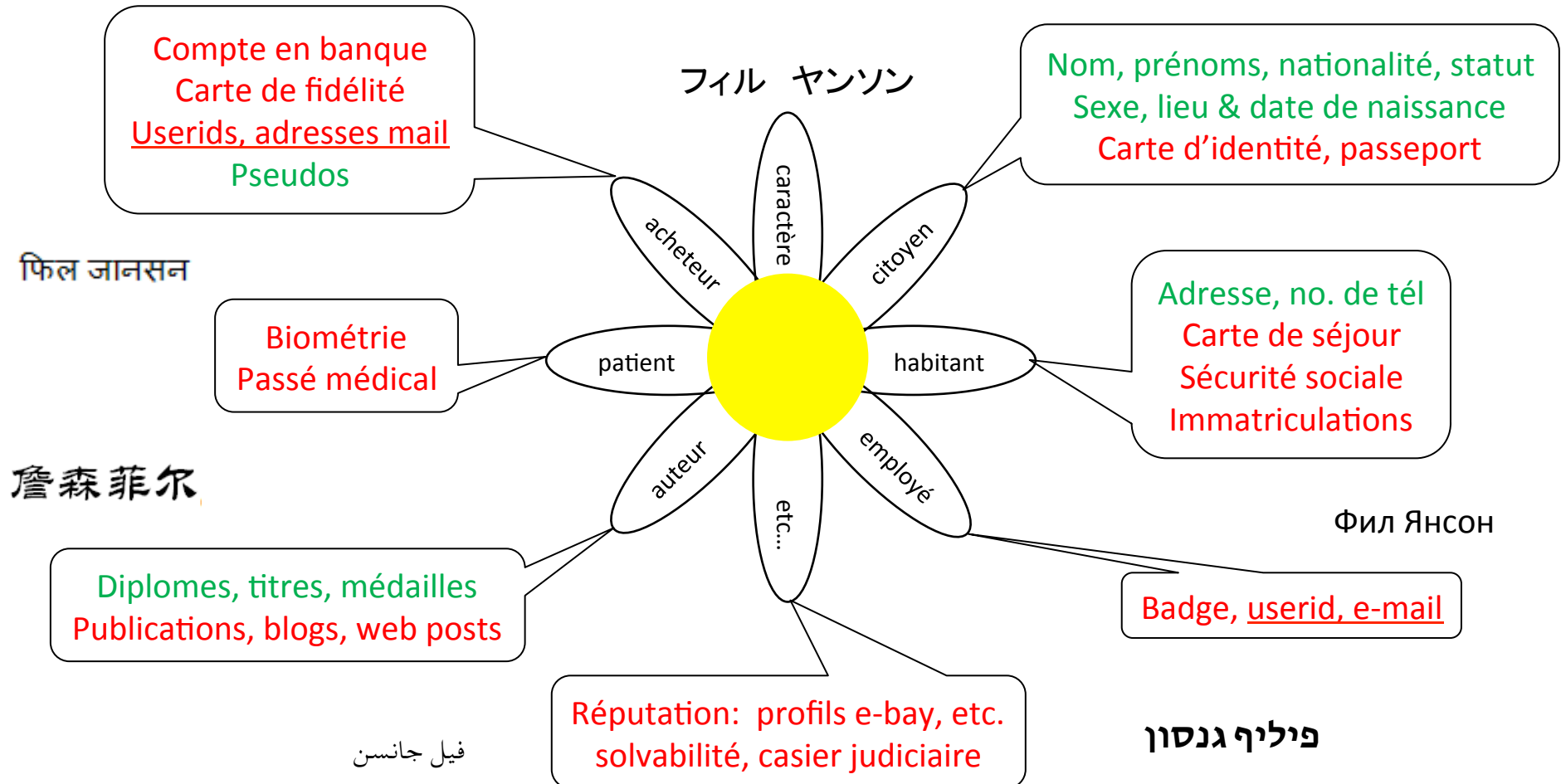
Son employeur

Son client

Son conjoint

Qu'est-ce qu'une identité (électronique) ?

Une énorme collection d'attributs (électroniques) **uniques** ou **communs** à plusieurs individus



Combien d'identités (et de mots de passe) ?

Une seule identité intégrée

Une multitude d'identités déconnectées

Un seul userid valable partout

Une multitude d'identifiants

Un seul mot de "passe-partout"

Une multitude de mots de passe

Grande facilité

Un cauchemar

Insécurité

Mais plus de sécurité

Aucune sphère privée

Une nécessité
pour la sphère privée

citoyen

habitant

employé

acheteur

patient

auteur




etc...

=> Trouver le bon compromis

Plan de la leçon

- ▶ Principes de base
- ▶ Confidentialité, intégrité et responsabilité : cryptographie
- ▶ Authentification
- ▶ **Autorisation**
 - ▶ contrôle d'accès
 - ▶ sécurisation des réseaux
 - ▶ calculs non autorisés : maliciels
- ▶ Règles de bonne conduite
- ▶ Résumé / Vue d'ensemble

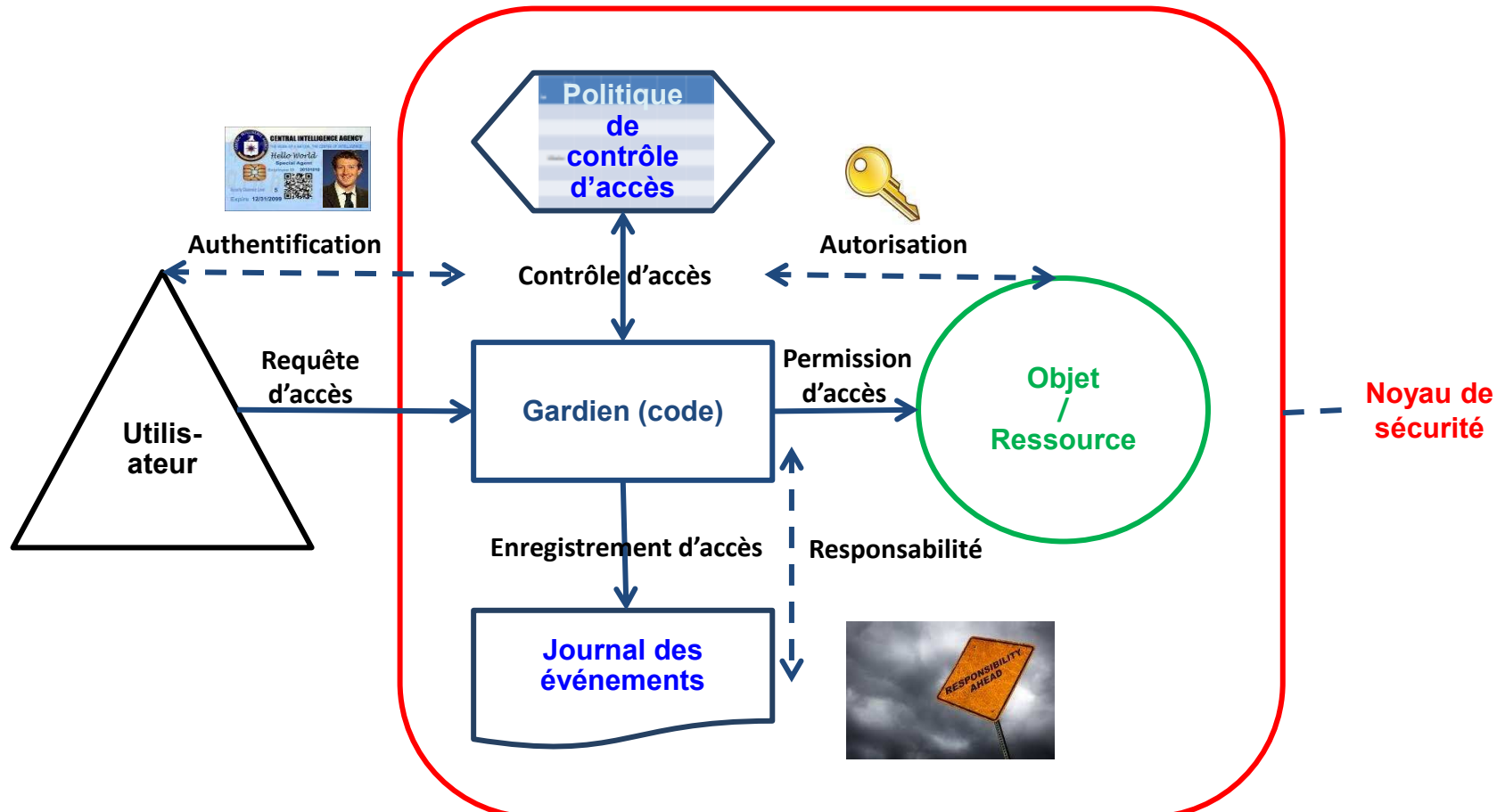
Autorisation – Politique de contrôle d'accès – Vue matricielle

Qui \ Quoi	O	B	J	E	Ts
	Logiciel	...	<u>Fichier</u>	...	Matériel
A ...			<div> <div>Permissions de l'acteur de lire / écrire / exécuter l'objet</div> <div>R/W/X...</div> <div>    </div> </div>		
C Logiciel					
T ...					
E <u>Utilisateur</u>					
U ...					
R Matériel					
S ...					
Sécurité de l'Information			Sécurité des Communications		Sécurité du Calcul
Autorisation			Maliciels		Meilleures pratiques

Liste de contrôle d'accès
associée à l'objet
wi

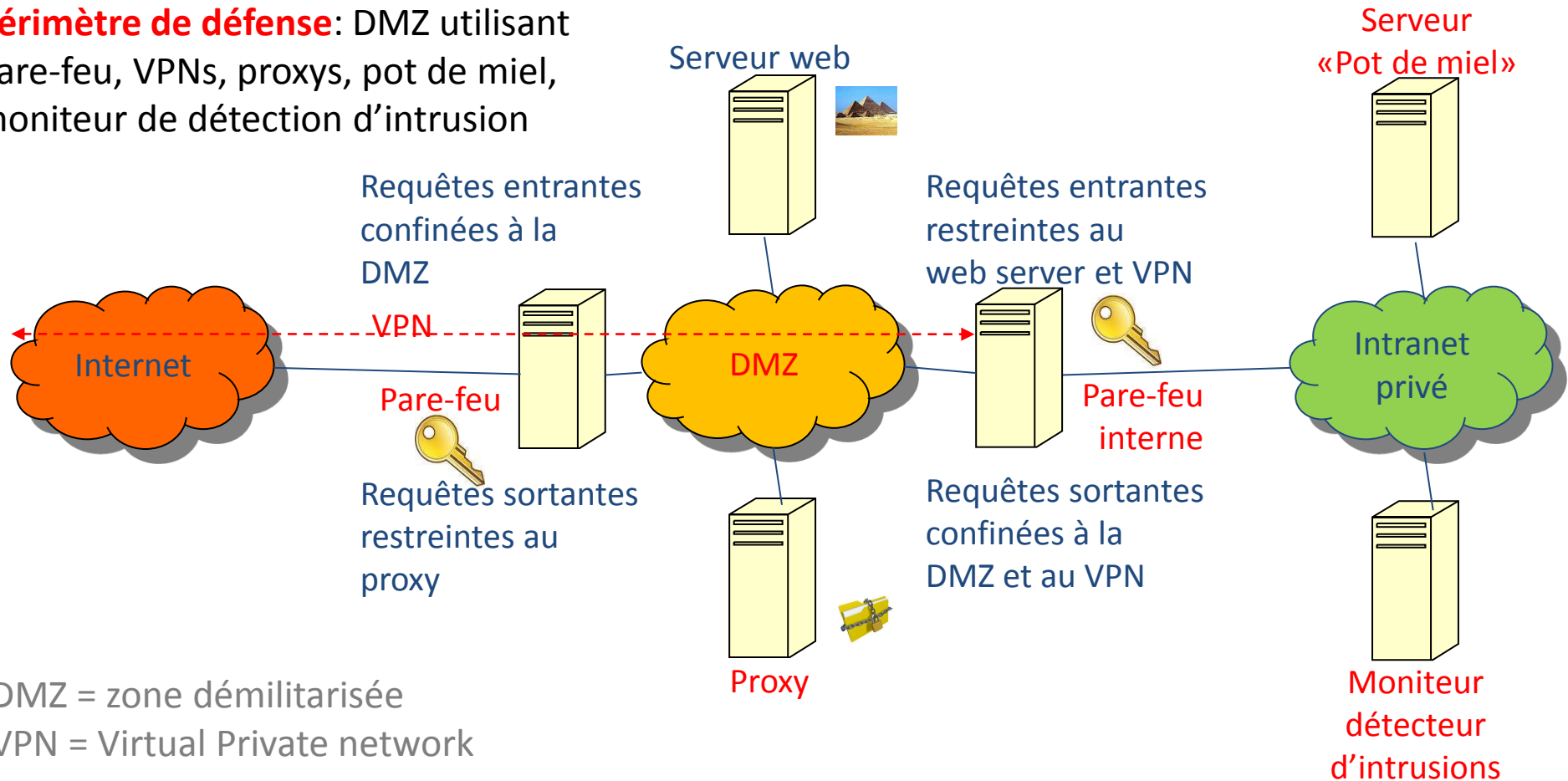
Autorisation – Modèle de système sécurisé

- Modifier logiciel ou données du **noyau de sécurité** exige les privilèges de “super-utilisateur”
- Ces privilèges de **super-utilisateur** ne sont accordés qu’au **noyau de sécurité**



Sécurité des réseaux

Périmètre de défense: DMZ utilisant Pare-feu, VPNs, proxys, pot de miel, moniteur de détection d'intrusion



DMZ = zone démilitarisée

VPN = Virtual Private network

Maliciels

L'essence de tout maliciel = la mobilité du logiciel

- Vecteurs
- Taxonomie



La seule solution absolue: “Trusted Computing”

Vecteurs de maliciel

- ▶ E-mails / spam / clés USB (manipulation sociale)
- ▶ Téléchargement intentionnel ou accidentel à partir de sites corrompus / douteux
- ▶ Piratage (= exploitant des vulnérabilités)
 - Contre authentification ou autorisation
 - Par injection de paramètres malveillants
- ▶ Téléchargement non-sécurisé / non-vérifié à partir de sites réputés mais contaminés
- ▶ Maliciel déjà installé au préalable

Complexité croissante
pour l'attaquant



Taxonomie de propagation des maliciels

- ▶ Cheval de Troie – maliciel caché **dans** un logiciel innocent
 - **Ne se propage pas** par lui-même et tend à rester caché
 - (Un “Oeuf de Pâques” est un cheval de Troie inoffensif)
- ▶ Virus – maliciel résidant **dans** un logiciel innocent
 - **Se propage** à d’autres logiciels ou médias et voyage avec eux
 - Sur une action de l’utilisateur (click, open, copy, install, etc.) pour causer une infection
- ▶ Ver – maliciel **indépendant** d’autres logiciels
 - **S’auto-propage** au gré des médias ou en exploitant des vulnérabilités via des réseaux



Plan de la leçon

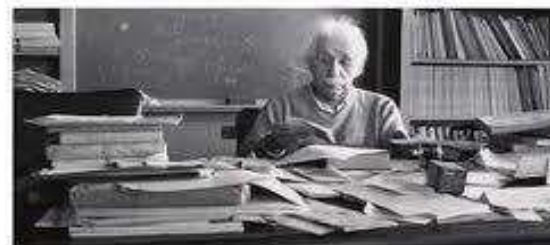
- ▶ Principes de base
- ▶ Confidentialité, intégrité et responsabilité : cryptographie
- ▶ Authentification
- ▶ Autorisation
- ▶ **Règles de bonne conduite**
- ▶ Résumé / Vue d'ensemble

Règles de conduite et bonnes pratiques

- ▶ Lieu de travail
- ▶ Postes de travail
- ▶ *Serveurs, applications, et bases de données*
- ▶ *Centres de traitement*

Meilleures pratiques – Lieu de travail

- ▶ Verrouiller les **systèmes portables** à la surface de travail
- ▶ Verrouiller / libérer / ramasser la sortie des **imprimantes**
- ▶ *Verrouiller puis déchiqueter les **documents et supports à éliminer***
- ▶ Verrouiller les **boîtes aux lettres internes**
- ▶ Imposer une politique de bureaux nets
 - Aucun **support** mémoire
 - Aucun **gadget** mobile*(Einstein n'a pas toujours raison!)*



"If a cluttered desk is a sign of a cluttered mind, Of what then is an empty desk a sign?"
~ Albert Einstein

Meilleures pratiques – Lieu de travail



► Interdire

- L'envoi automatique de **notices d'absence** – c'est une invitation au spam
- Le **reroutage** de mails professionnels sur un compte privé
- L'usage de **postes de travail publics** à des fins professionnelles
- L'usage de **services publics** à des fins professionnelles
e.g. Google Docs/Drive, calendar, contacts, iCloud, etc.

► En voyage dans des pays réputés "à risque"

- Emporter un **ordinateur portable "vierge"** et reformatter son disque au retour
- Eteindre **micros et cameras** (téléphone portable!) pendant les meetings critiques
- Ne **jamais taper de mots de passe** – les copier/coller à partir d'un stick USB



Meilleures pratiques – Poste de travail / téléphone portable

- ▶ Installer **anti-virus et pare-feu personnel**
 - Toujours se connecter via un routeur et pas directement au fournisseur de service
- ▶ Appliquer systématiquement tous les “**patches**” offerts par les fabricants de logiciels
 - Ne jamais accepter **un patch de logiciel quand on est connecté à un Wi-Fi public**
- ▶ Contrôler les paramètres **Bluetooth and Wi-Fi**
 - Bloquer l’administration d’un point d’accès Wi-Fi par son interface sans fil
- ▶ *Condamner les ports **USB et autres***
- ▶ Condamner le partage de **fichiers et imprimantes**
- ▶ Condamner **l’assistance à distance**
- ▶ **Crypter les disques (TrueCrypt / BitLocker) + verrouiller les écrans de veille**
 - Exiger un mot de passe de réveil sur tous les gadgets portables
- ▶ Faire des copies de **sauvegardes** régulières
 - Vérifier régulièrement **l’intégrité des fichiers** (p.ex. avec AIDE)
- ▶ Ne jamais exécuter d’application en **mode privilégié** (administrateur)
 - Ne télécharger que des **applications signées**
=> Des portables déverrouillés (= “**jailbroken**”) sont inacceptables
- ▶ Installer <http://preyproject.com/> pour pouvoir localiser un portable volé




Meilleures pratiques – Poste de travail / téléphone portable

- ▶ Imposer des règles de **sélection de mots de passe** strictes (v. authentification)
 - **NE JAMAIS** révéler aucun mot de passe à personne en aucune circonstance
- ▶ Forcer une déconnexion automatique (“time-outs”) en cas d’inactivité – **Max. 15 minutes**
- ▶ Ne faire tourner les *applications critiques que sur des postes dédiés* à cette fin
- ▶ Interdire le *partage de poste professionnel / financier* avec des proches
- ▶ Écraser / reformater / déchiqueter **tout support mémoire ou poste décommissionné**
 - Des dommages considérables résultent de portables revendus ou jetés tels quels



Meilleures pratiques – Navigation



- ▶ Exploiter les **plug-ins de sécurité** pour les navigateurs
 - ▶ Faire tourner le navigateur en **mode privé**
 - ▶ N'accepter que sélectivement les **scripts** (Activex, Javascript, etc.) 
 - ▶ N'accepter que sélectivement les **cookies**
 - ▶ Purger régulièrement les pseudo-cookies Adobe Flash (**LSOs**)
 - ▶ Condamner les **fonctions "auto-complete"** pour les formulaires sensibles
 - ▶ Ne jamais envoyer d'informations sensibles via un **URI**
 - ▶ Naviguer via un **proxy** (v. planche suivante)
- ▶ Logout – ne pas compter sur les déconnexions automatiques ("time-outs")

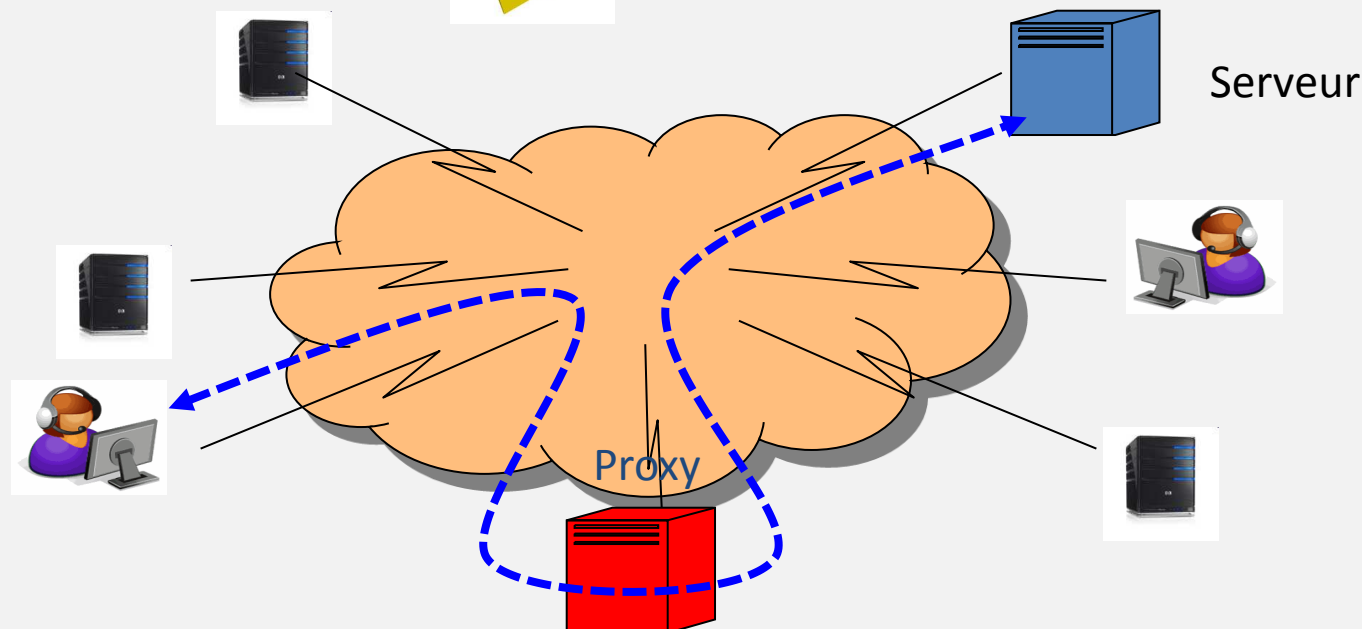
Meilleures pratiques – Navigation via proxy

► Un proxy de navigation sécurisé inclut

- Un **senseur d'interférence avec le clavier** pour bloquer les maliciels d'espionnage
- Le **cryptage des fichiers et connections**
- Un **filtre anti-virus**

► Cette solution **empêche un maliciel d'accéder** aux informations privées sur le poste de travail assurant ainsi une **résistance aux attaques** de sites contaminés

► Elle rend toutes les **sessions anonymes**



Sécurité Facebook

- ▶ Utiliser tous les réseaux sociaux via un **navigateur séparé et confiné**
 - **Sur un ordinateur (les tablettes et smartphones sont insuffisamment protégés)**
- ▶ Inscription Facebook : ne **JAMAIS** utiliser la fonction “Trouver des amis”
 - **Elle transfère tout votre carnet d'adresses à Facebook !**
- ▶ Les contrôles de sécurité / sphère privée de Facebook sont **éparpillés partout** pour les compliquer
- ▶ L'option “**A propos de**” devrait être “**Amis**” **uniquement** pour toutes les catégories
- ▶ L'option “**Amis**” devrait être “**Amis**” de telle sorte que seuls vos amis se voient les uns les autres
- ▶ **Le contrôle d'accès** est au-delà de la compréhension d'un utilisateur normal
- ▶ Souvenez-vous: même après fermeture d'un compte, des **copies peuvent survivre pour toujours**
 - **Copies de sauvegarde, copies archivées par des tiers, etc.**

Voir excellentes directives Facebook du Canton de Zurich (en allemand)

- https://dsb.zh.ch/internet/datenschutzbeauftragter/de/ueber_uns/veroeffentlichungen/leitfaeden_und_checklisten/_jcr_content/contentPar/publication_1/publicationitems/titel_wird_aus_dam_e/download.spooler.download.1359360790285.pdf/Checkliste+Privacy+Facebook.pdf

Quelques bons conseils pratiques

- ▶ Se méfier des **postes de travail et services publics** – surtout gratuits
- ▶ Se méfier de **pirates en des lieux publics** – surtout réputés “à risque”
- ▶ Se méfier des **logiciels-espions** – micros et webcams télécommandées

- ▶ Toujours sécuriser son **Wi-Fi**
- ▶ Toujours activer **anti-virus et pare-feu**
- ▶ Toujours “**patcher**” ses logiciels

- ▶ Bien choisir et ne jamais révéler ses **mots de passe**
- ▶ Ne jamais travailler en mode “**administrateur**”
- ▶ Se **détacher** après toute session de travail ou délai inactif

- ▶ Faire des copies de **sauvegarde** régulières
- ▶ **Encrypter** tous ses supports-mémoires
- ▶ **Détruire** tout support mémoire ou papier en fin de vie

“Clean desk”: Ne jamais laisser trainer équipements ou supports-mémoires portables (Einstein n’a pas toujours eu raison!)



"If a cluttered desk is a sign of a cluttered mind, Of what then is an empty desk a sign?"
- Albert Einstein

Plan de la leçon

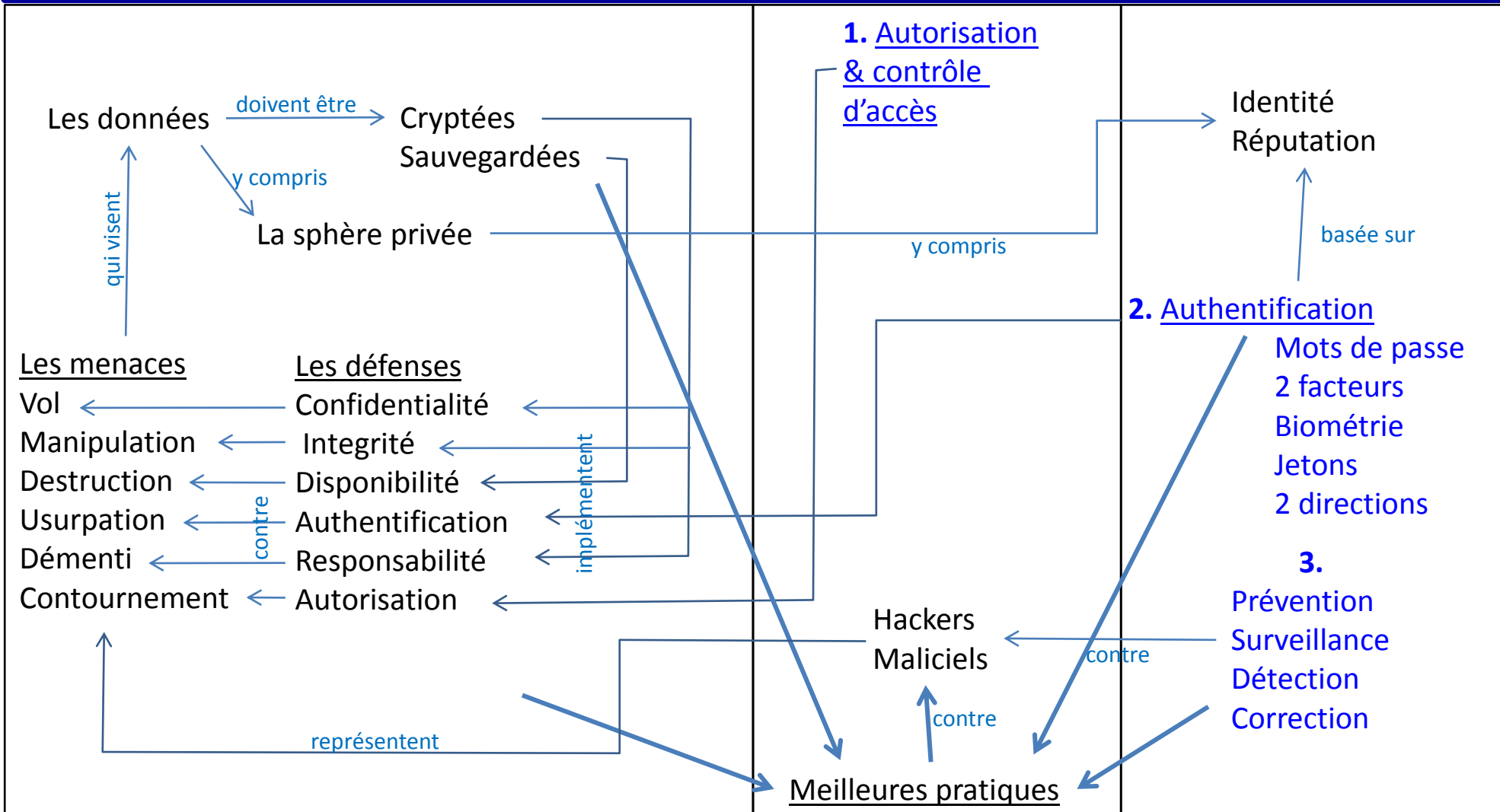
- ▶ Principes de base
- ▶ Confidentialité, intégrité et responsabilité : cryptographie
- ▶ Authentification
- ▶ Autorisation
- ▶ Règles de bonne conduite
- ▶ **Résumé / Vue d'ensemble**

Dans le rétroviseur ...

Information

Computing

Communications



Conclusion

- ▶ Savoir identifier les menaces et connaître les niveaux de défense appropriés
la sécurité totale n'existe pas !
- ▶ Sauvegardez, cryptez vos données
 - ▶ One-Time Pad, DES, AES
 - ▶ RSA, courbes elliptiques
- ▶ Choisissez bien, changez et protégez vos mots de passe
- ▶ D'une façon générale, adoptez de meilleures pratiques en vue d'une plus grande sécurité

Ceci termine ce cours I.C.C. !

En espérant que ce « voyage » annoncé dans la toute première leçon vous a

- ▶ plu, intéressé, instruit, ...