

# Information, Calcul et Communication

## Module 3 : Systèmes

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

Ph. Janson

## I – Sécurité de l'Information

### ▶ I – Sécurité de l'Information

- Principes de base
- Menaces
- Défenses
- Protection de la sphère privée
- Sécurisation de l'information

### ▶ C – Sécurité des Communications

### ▶ C – Sécurité du Calcul

### ▶ Environnementales (probabilité marginale)

- Catastrophes naturelles

### ▶ Humaines

#### ▪ Internes

- Les erreurs (environ 50% des cas)
- Les abus de privilèges (environ 20% des cas)

#### ▪ Externes (environ 30% des cas)

- La manipulation sociale
  - Par mail ou web (spam, spim, spit, phishing, whaling, vishing, pharming)
  - Par réseaux sociaux
- Les attaques physiques

### ▶ Techniques

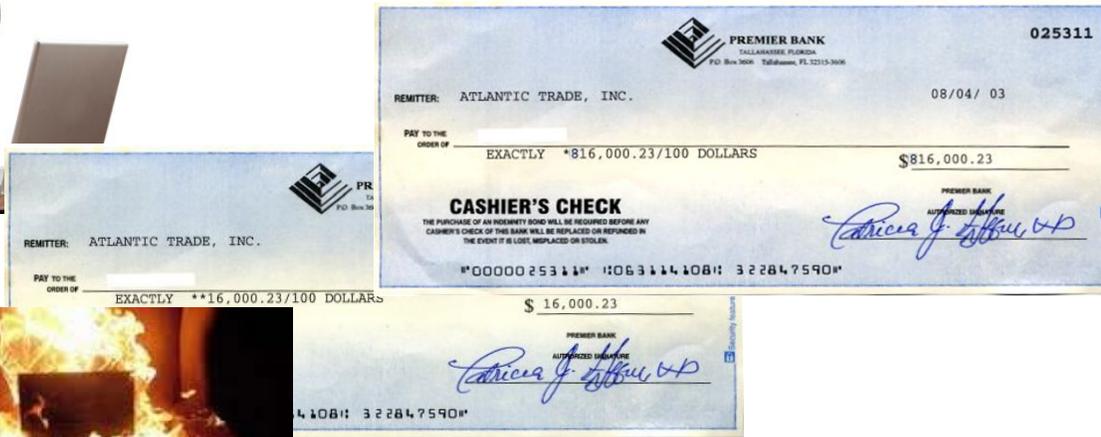
- Les attaques informatiques par des pirates
  - Par exploitation de **vulnérabilités** logicielles
- Les maliciels = logiciels malveillants
  - Les **chaînes de production** contaminées

# Menaces

► Le vol



► La manipulation



► La destruction



► Le démenti

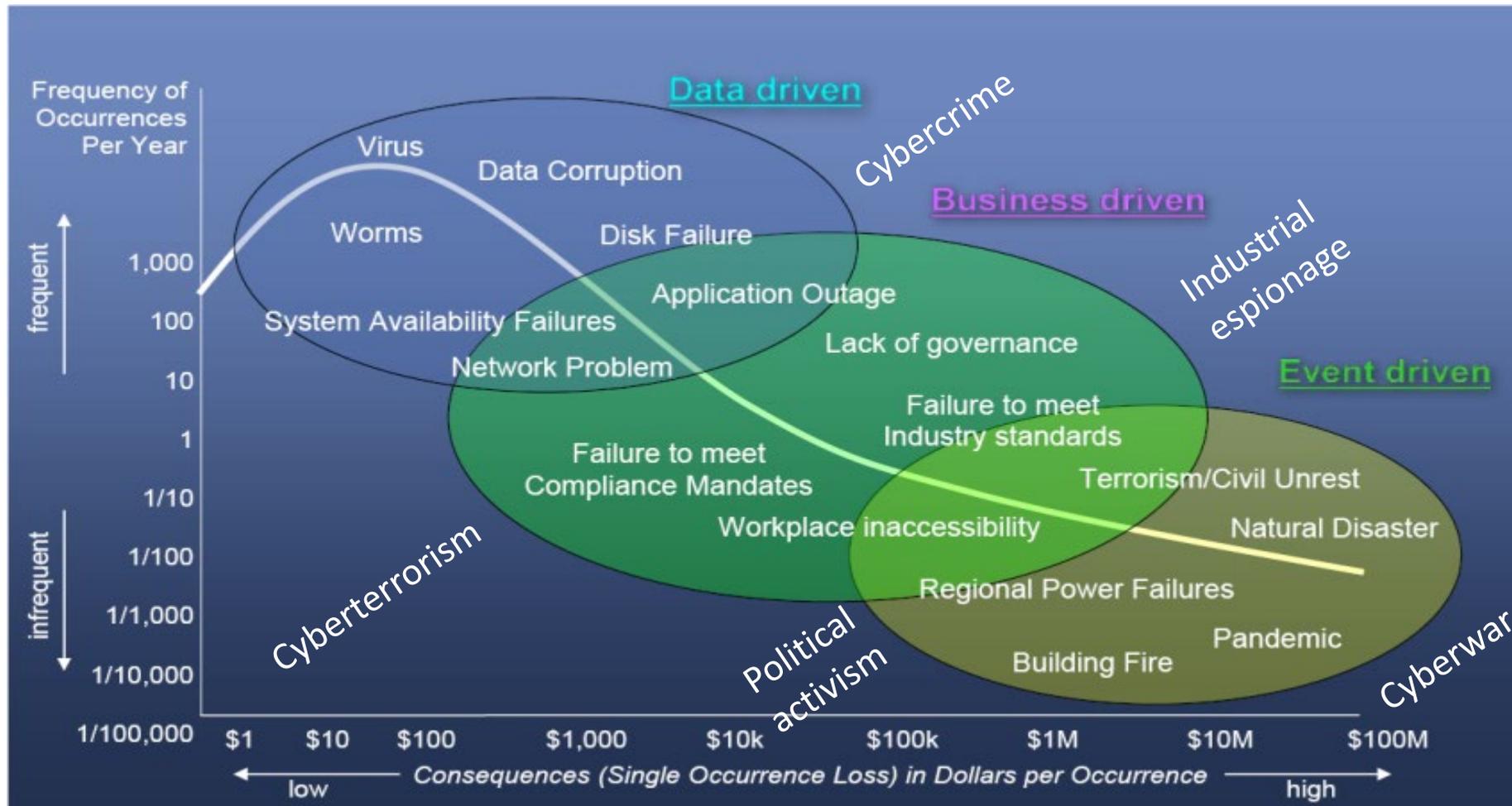


► L'usurpation d'identité



► Le contournement de défenses

# Menaces – Réalité et ampleur



Reprinted by courtesy of International Business Machines Corporation,  
© (2008-2009) International Business Machines Corporation

Source: IBM Security Technology Outlook 2008

# Défenses

## L'ultime objectif: Contrôler qui a quel droit

Les menaces étaient

- ▶ Le vol d'informations
- ▶ La manipulation
- ▶ La destruction
- ▶ Le démenti
- ▶ L'usurpation d'identité
- ▶ Le contournement de défenses

Les combattre exige

- ▶ Confidentialité
- ▶ Intégrité
- ▶ Disponibilité
- ▶ Responsabilité
- ▶ Authentification
- ▶ Autorisation



# Sensibilisation à la sécurité de la sphère privée

## ► Confidentialité de notre identité

- ⇒ Isoler ses différentes facettes contre l'usurpation
- ⇒ **PAS** dissimuler des facettes répréhensibles
- ⇒ **Frontière** entre responsabilité et sphère privée

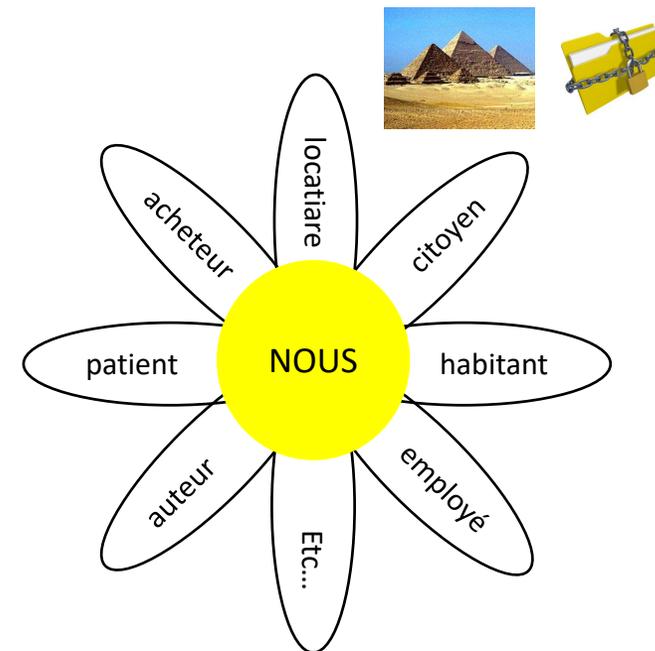
## ► Intégrité de notre réputation

- ⇒ Durement gagnée, facilement ruinée

+ **Obligations** pour les récipiendaires de nos informations privées

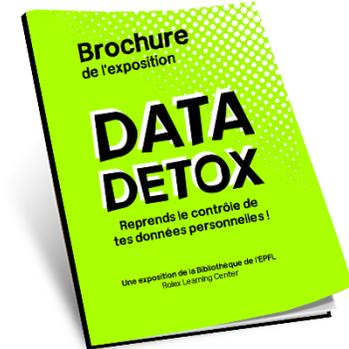
## ► Règlement général sur la protection des données / GDPR (UE / mai 2018)

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



# Sensibilisation à la sécurité de la sphère privée

- ▶ De plus en plus de données électroniques (privées) sont
  - **Récoltées**
  - **Stockées** pour toujours on ne sait où dans un “cloud”
  - **Échangées**
  - **Analysées** par corrélation entre sites
  - **Publiées**
  
- ▶ Par des tiers dont le **fond de commerce est l’invasion et la commercialisation** de notre sphère privée
  - **politiques confuses et mensongères** concernant nos données privées
    - “**opt-out**” plutôt que “**opt-in**”
  
- ▶ Méfiez-vous des services “gratuits” → c’est “nous” la marchandise
  - Nous ignorons les conséquences de la vie dans un monde qui n’oublie plus jamais rien



→ [Brochure de l'exposition Data Detox \(EPFL 30.08-25.10.2018\)](#)

# Sécurisation de l'information

## ► Disponibilité



## ► Cryptage

### ▪ Confidentialité



### ▪ Intégrité



**Outils pour obtenir des garanties  
sur la véracité des contenus  
et sur leur origine**

### ▪ Responsabilité (“signature digitale”)



## Sécurisation de l'information – 1) Disponibilité / robustesse

▶ Menace = perte / inaccessibilité / destruction de l'information

▶ Défense = sauvegarde

▶ Mécanisme = copie(s)

▶ Implémentation

▪ Nombre de copies	1	2	3	...	N
▪ Localisation des copies:		adjacentes			distantes
▪ Fréquence des copies	/mois	/semaine		/jour	/heure temps réel
▪ Coût des copies	minimal				substantiel

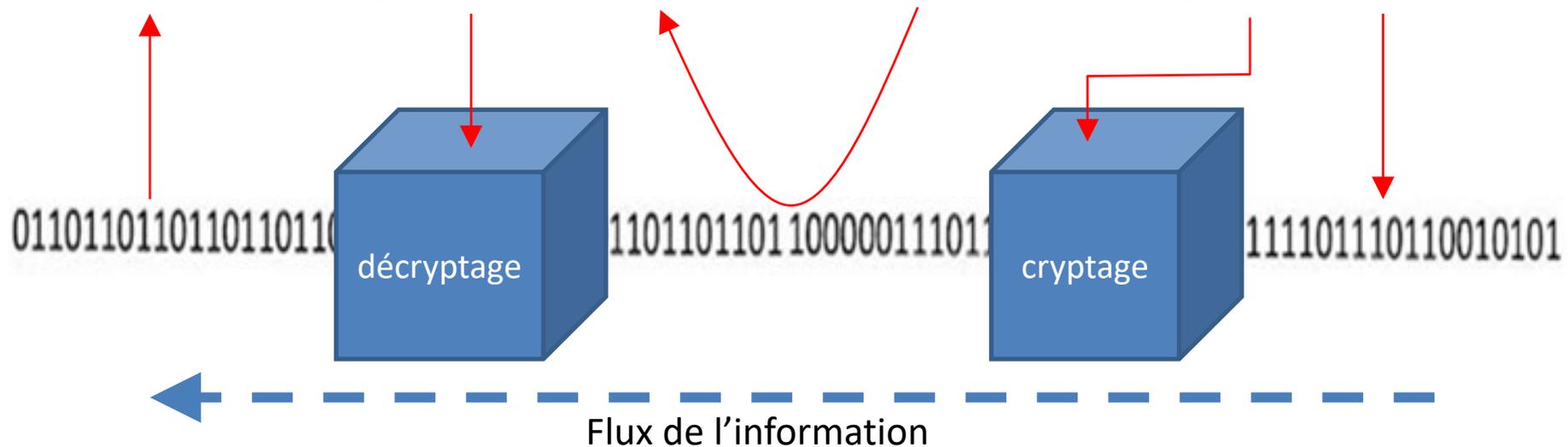
▶ Pour des raisons de protection de la sphère privée on peut préférer un serveur local (switch) plutôt que les géants de l'Internet sujets à une législation étrangère (Google, Microsoft, Apple, etc) telle que le [cloud act depuis 2018](#).

**NB: la préservation pérenne de média extrêmement volumineux est incertaine – trop gros pour tester**



## Sécurisation de l'information – 2) Confidentialité

- ▶ Menace = vol d'information
- ▶ Mécanisme de défense = confidentialité (indiquée par l'icône  dans les navigateurs)
- ▶ Implémentation = cryptographie
- ▶ Principe  
information = décryptage (clé, cryptogramme) / cryptogramme = cryptage (clé, information)



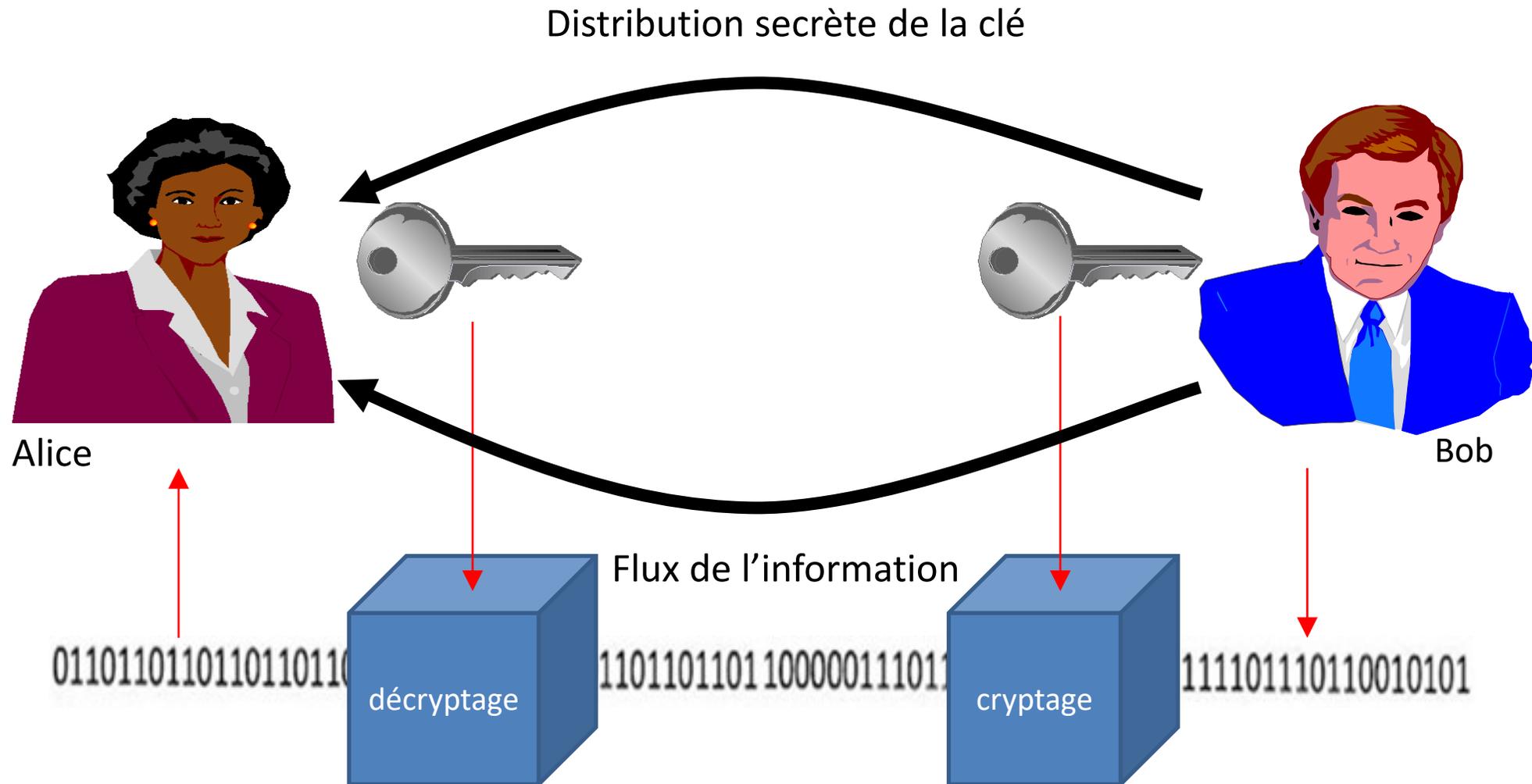
- ▶ Il existe deux familles d'algorithmes cryptographiques: **symétriques** et **asymétriques**

# Cryptographie symétrique à clés secrètes partagées



- ▶ La clé de décryptage est la **même** que la clé de cryptage
- ▶ Cette clé doit donc rester **secrète** pour protéger la confidentialité
- ▶ Elle doit être **partagée** entre les personnes encryptant et décryptant l'information
  
- ▶ Exemples: XOR, DES, 3DES, AES

# Confidentialité par cryptographie symétrique



SpeakUp: the C++ bitwise operator XOR is denoted by the symbol  $\wedge$

```
int x1 (12) , x2 (9) ;
```

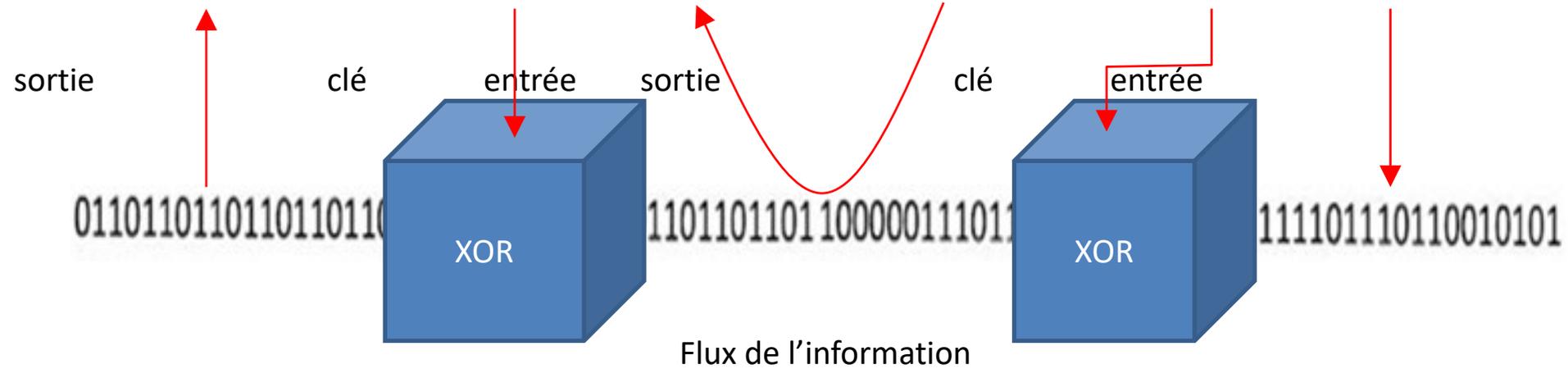
What is the value of the expression :  $(x1 \wedge x2) \wedge x2$

- A. Produit Exp( $x1 * x2$ ) avec une violation du domaine couvert
- B.  $x1$
- C.  $x2$
- D. Une valeur différente des autres réponses

# Exemple – XOR



information = XOR (clé, cryptogramme) / cryptogramme = XOR (clé, information)



Flux de l'information

Bit d'entrée	Bit de clé	Bit de sortie
0	0	0
0	1	1
1	0	1
1	1	0

## Exemple – XOR



Soit **b** un bit de donnée (b vaut 0 ou 1)

Le bit de la clef ne peut prendre que 2 valeurs : **0** ou **1**

Le bit de la clef vaut **0**

CRYPTAGE:

**b** xor **0** donne **b**

DECRYPTAGE:

**b** xor **0** donne **b**

On obtient bien le bit  
d'origine **b**

Le bit de la clef vaut **1**

CRYPTAGE:

**b** xor **1** donne **not b**

DECRYPTAGE:

**(not b)** xor **1** donne **not (not b) = b**

On obtient bien le bit  
d'origine **b**

## Exemple – XOR



► N bits d'information    XOR    N bits de clé

Info	1	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	0	1	0
Clé	0	1	1	1	0	1	1	0	1	0	1	0	1	1	0	0	0	1	0
Crypto	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	1	0	0	0

Crypto	1	1	0	0	0	1	1	1	0	0	0	1	1	1	0	1	0	0	0
Clé	0	1	1	1	0	1	1	0	1	0	1	0	1	1	0	0	0	1	0
Info	1	0	1	1	0	0	0	1	1	0	1	1	0	0	0	1	0	1	0

■ Problème: longueur de clé = longueur de l'information

## Exemple – XOR



► N bits d'information    XOR    8 bits de clé

Info	1	0	1	1	0	0	0	1	=	1	0	1	1	0	0	0	1		0	1	0
Clé	0	1	1	1	0	1	1	0		0	1	1	1	0	1	1	0		0	1	1
Crypto	1	1	0	0	0	1	1	1	=	1	1	0	0	0	1	1	1		0	0	1

Crypto	1	1	0	0	0	1	1	1	=	1	1	0	0	0	1	1	1		0	0	1
Clé	0	1	1	1	0	1	1	0		0	1	1	1	0	1	1	0		0	1	1
Info	1	0	1	1	0	0	0	1	=	1	0	1	1	0	0	0	1		0	1	0

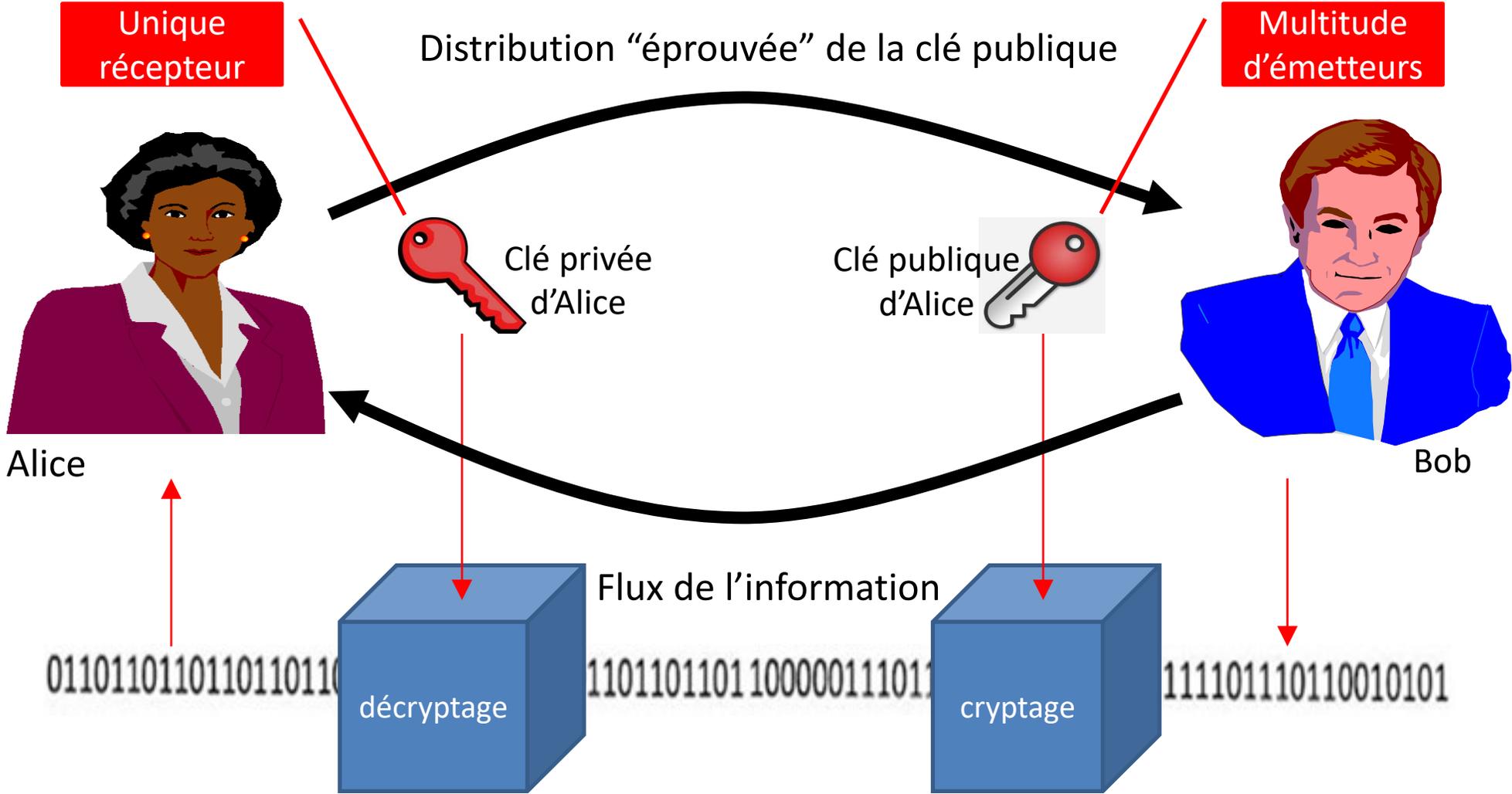
Problème: même octet d'information => même octet de cryptogramme  
=> **cryptanalyse!**

En pratique: clés aussi longues que possible => 128 ... 4096 bits



- ▶ La clé de décryptage et la clé de cryptage sont **différentes**
- ▶ La clé de décryptage est **privée** (secrète)
- ▶ La clé de cryptage est **publique** (pas du tout secrète)
  
- ▶ Exemples: RSA (Rivest – Shamir – Adleman)

# Confidentialité par cryptographie asymétrique



# RSA: Comment construire / utiliser la paire clef-publique / clef-privée

On veut envoyer un message crypté à Alice

1. Prendre deux grands nombres premiers  $p$  et  $q$
2.  $n = p \cdot q$
3.  $\varphi(n) = (p-1)(q-1)$
4. choisir  $e$  tel que  $\text{pgcd}(\varphi(n), e) = 1$

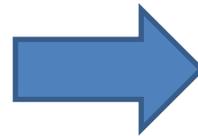


Clef publique =  $(n, e)$



**Emetteur: Bob** / message  $m$  tel que  $m < n$

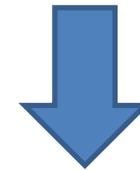
6. Message crypté  $M = m^e \text{ modulo } (n)$



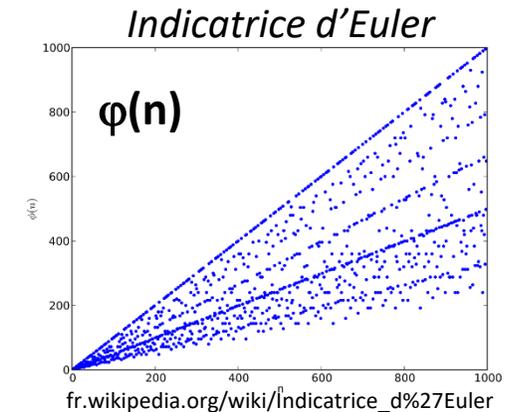
**Destinataire: Alice** reçoit  $M$

5. Calcul de  $d$  tel que  $(d \cdot e) \text{ modulo } (\varphi(n)) = 1$

Clef privée =  $d$



7. Message décrypté  $m = M^d \text{ modulo } (n)$



# RSA: pourquoi ça marche ?

$p$  et  $q$  étant deux grands nombres premiers il est très difficile de les retrouver à partir de  $n$

$$m^{\varphi(n)} \text{ modulo } n = 1 \quad // \text{ Théorème d'Euler-Fermat}$$

Sachant que que  $(d.e) \text{ modulo } (\varphi(n)) = 1$  on peut écrire  $(d.e) = k. \varphi(n) + 1$

Décryptage: calculer  $X = M^d \text{ modulo } (n)$  or  $M = m^e \text{ modulo } (n)$

$$\text{donc } X = (m^e)^d \text{ modulo } (n)$$

$$X = m^{d.e} \text{ modulo } (n)$$

$$X = m^{k. \varphi(n) + 1} \text{ modulo } (n)$$

$$X = m^{k. \varphi(n)} m \text{ modulo } (n)$$

$$X = (m^{\varphi(n)})^k . m \text{ modulo } (n)$$

$$X = ((m^{\varphi(n)})^k \text{ modulo } n) . (m \text{ modulo } (n))$$

On applique  $k$  fois le  
théorème d'Euler-Fermat



1.1.1....1

$m$

# RSA: un exemple concret

Destinataire: Alice

$$p = 3$$

$$q = 11$$

$$n = 33$$

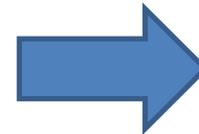
$$\varphi(n) = 2 \cdot 10 = 20$$

$e=7$  sans diviseur commun avec 20

D'où  $d=3$  car  $3 \cdot 7 = 21$  et  $21 \bmod 20 = 1$

Message de Bob :  $m = 9 < 33$

Message crypté  $M = 9^7 = 4782969 \bmod 33 = 15$



Alice reçoit 15



Message décrypté:  $15^3 = 3375 \bmod 33 = 9$

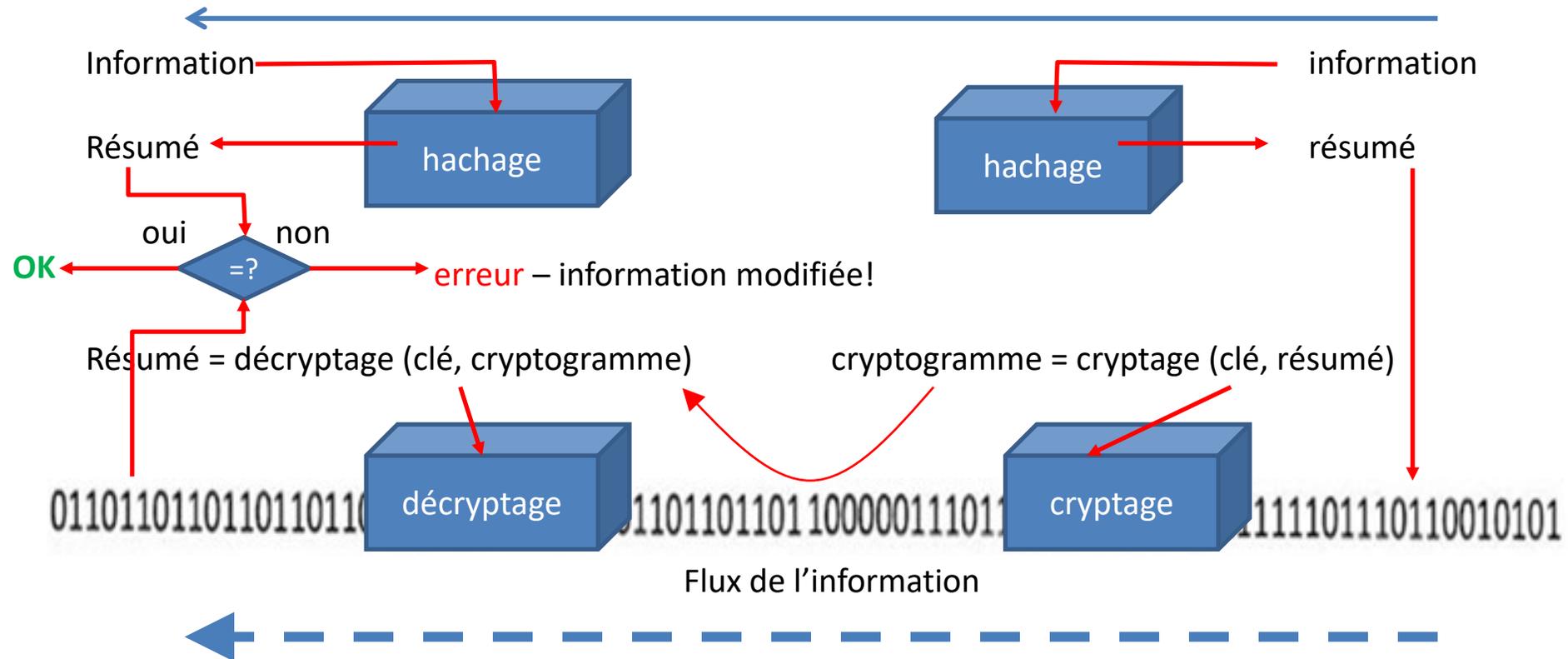
# Sécurisation de l'information – 3) Intégrité

To hash [Merriam-Webster]

1a : to chop (food, such as meat and potatoes) into small pieces

b : confuse, muddle

- ▶ Menace = modification d'information
- ▶ Mécanisme de défense = intégrité
- ▶ Implémentation = cryptographie
- ▶ Principe = l'information n'est pas confidentielle et ne doit donc pas (nécessairement) être cryptée



# Exemple de fonction de hachage : MD5 [Rivest 1991]

Historiquement important mais n'est plus utilisé

Produit un résumé/empreinte de **128 bit**  
pour n'importe quelle longueur de message

Le calcul du résumé est *irréversible*

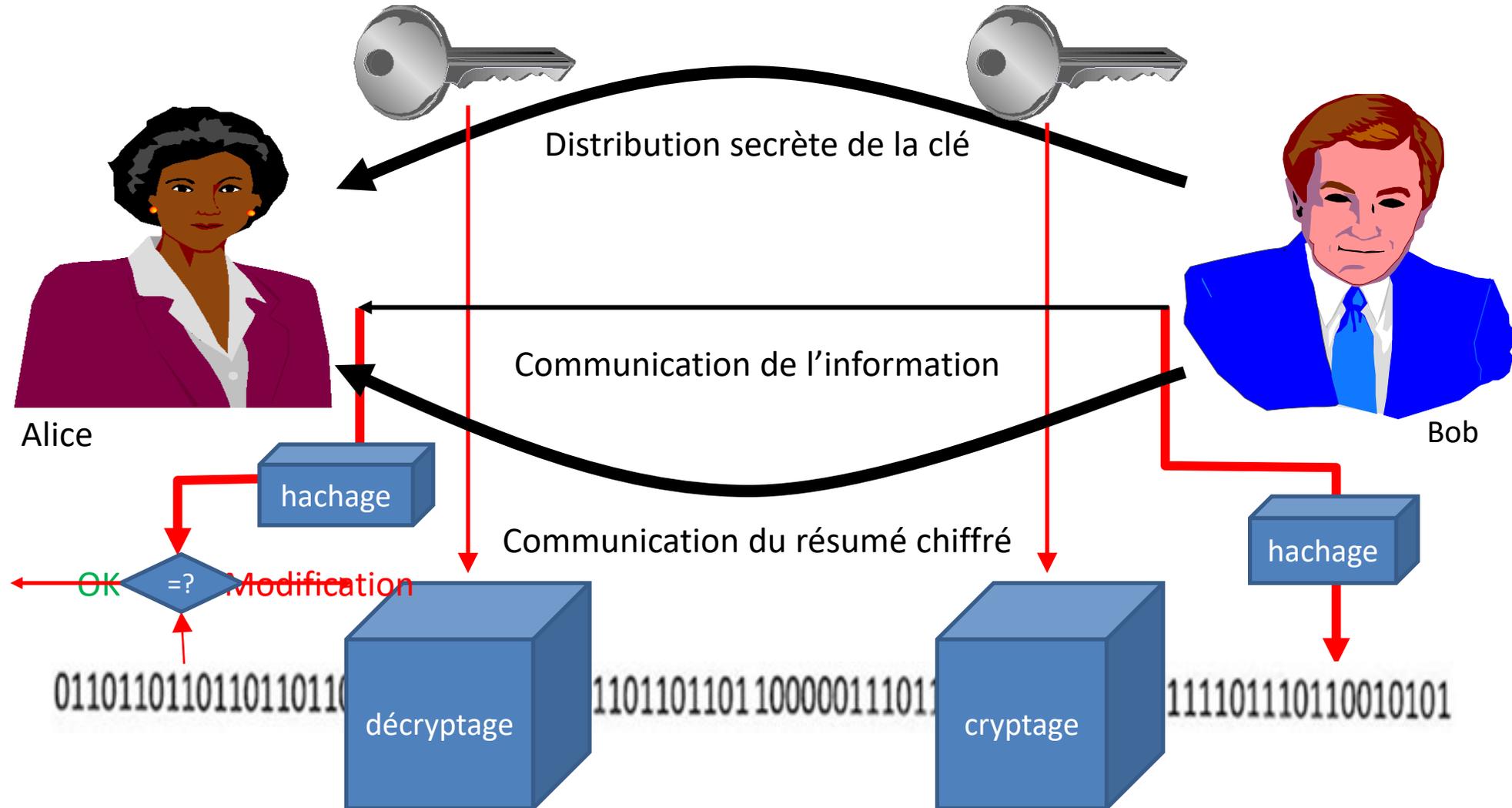
Le changement d'un seul caractère du  
message change radicalement l'empreinte:

En théorie la probabilité que deux messages  
différents mènent au même résumé est infime.

Ce cas est appelé une *collision* ; proba =  $1/2^N$  ou  
N est le nombre de bits du résumé.

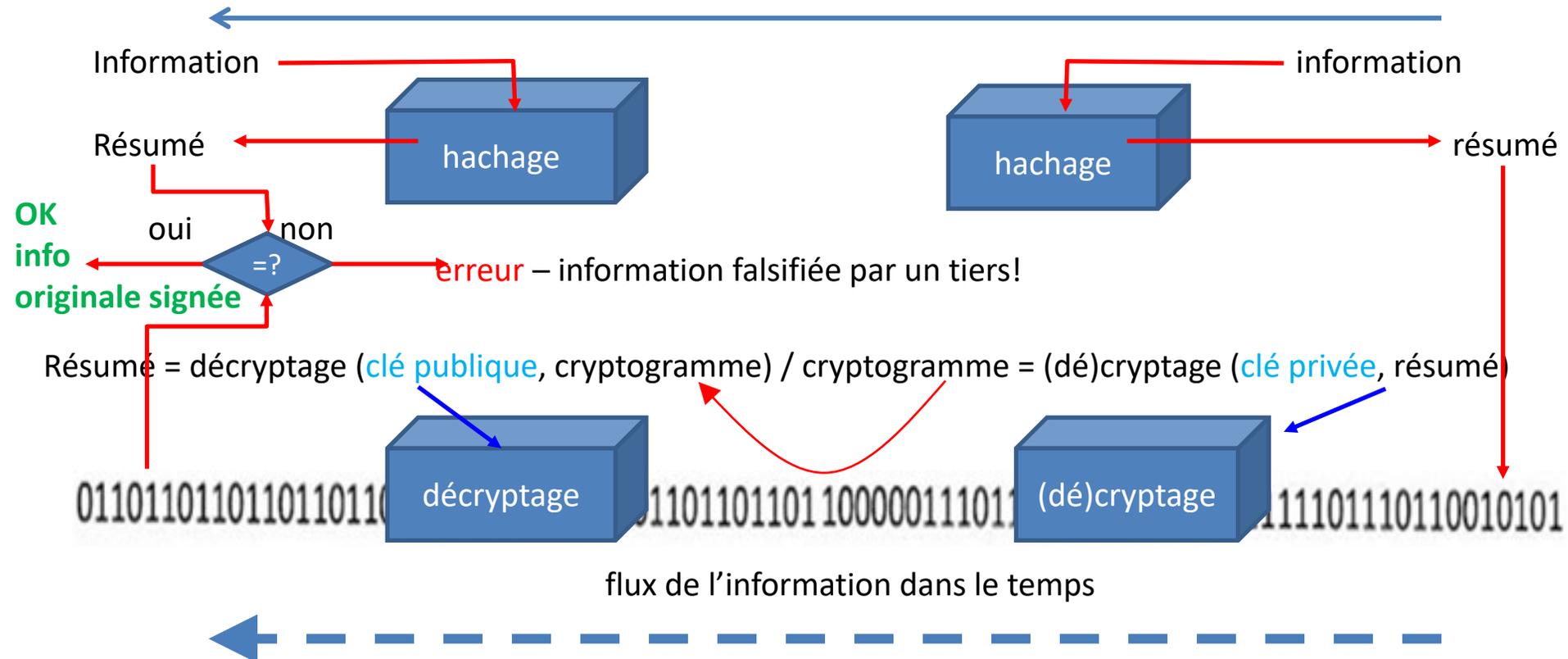
```
pour i de 0 à 63 faire
  si 0 ≤ i ≤ 15 alors
    f := (b et c) ou ((non b) et d)
    g := i
  sinon si 16 ≤ i ≤ 31 alors
    f := (d et b) ou ((non d) et c)
    g := (5×i + 1) mod 16
  sinon si 32 ≤ i ≤ 47 alors
    f := b xor c xor d
    g := (3×i + 5) mod 16
  sinon si 48 ≤ i ≤ 63 alors
    f := c xor (b ou (non d))
    g := (7×i) mod 16
  fin si
  var entier temp := d
  d := c
  c := b
  b := leftrotate((a + f + k[i] + w[g]), r[i]) + b
  a := temp
fin pour
```

# Intégrité par cryptographie symétrique

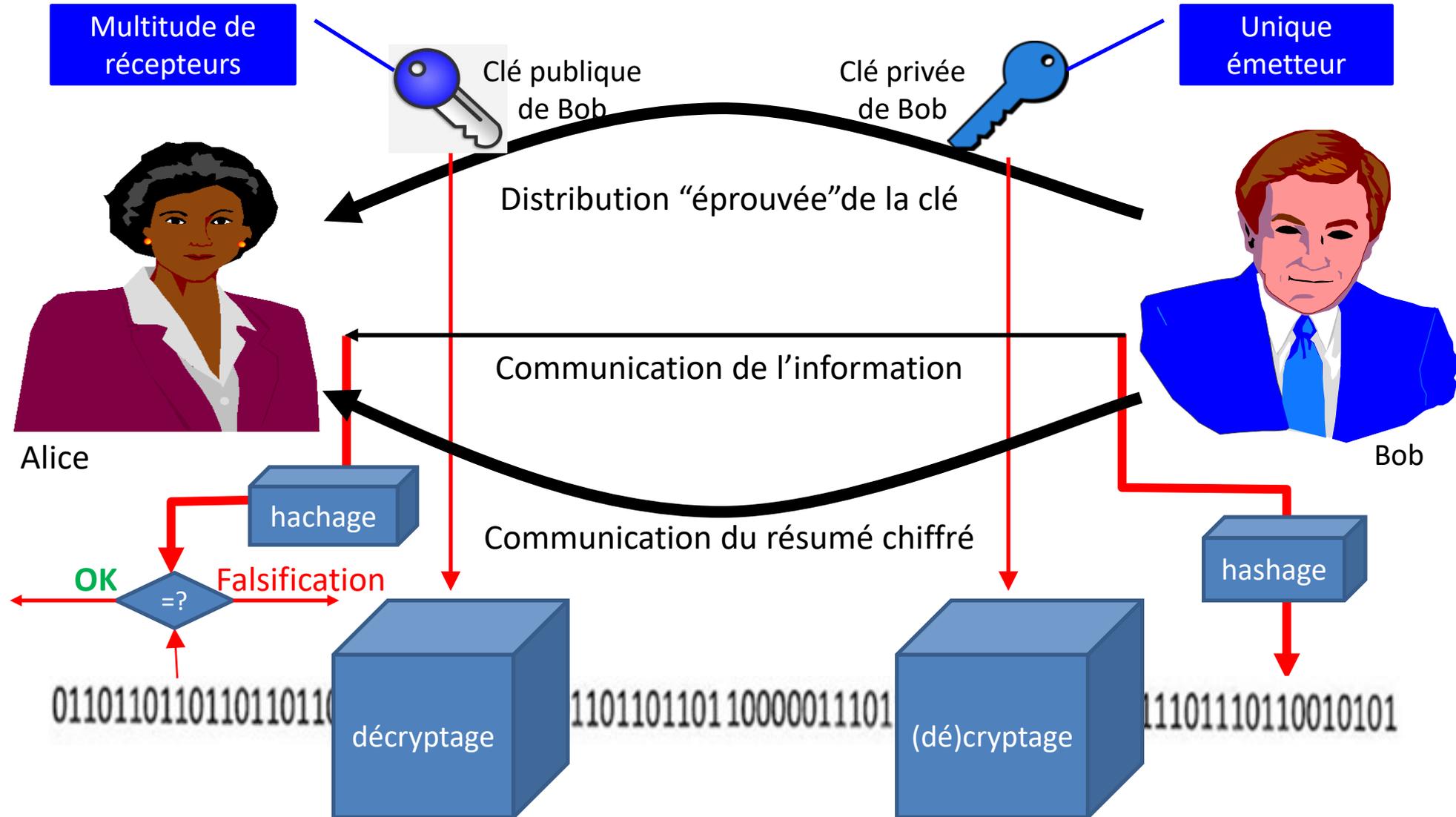


## Sécurisation de l'information – 4) Responsabilité

- ▶ Menace = démenti
- ▶ Mécanisme de défense = responsabilité
- ▶ Implémentation = signature numérique par cryptographie asymétrique
- ▶ Principe = l'information n'est pas confidentielle et ne doit donc pas (nécessairement) être cryptée

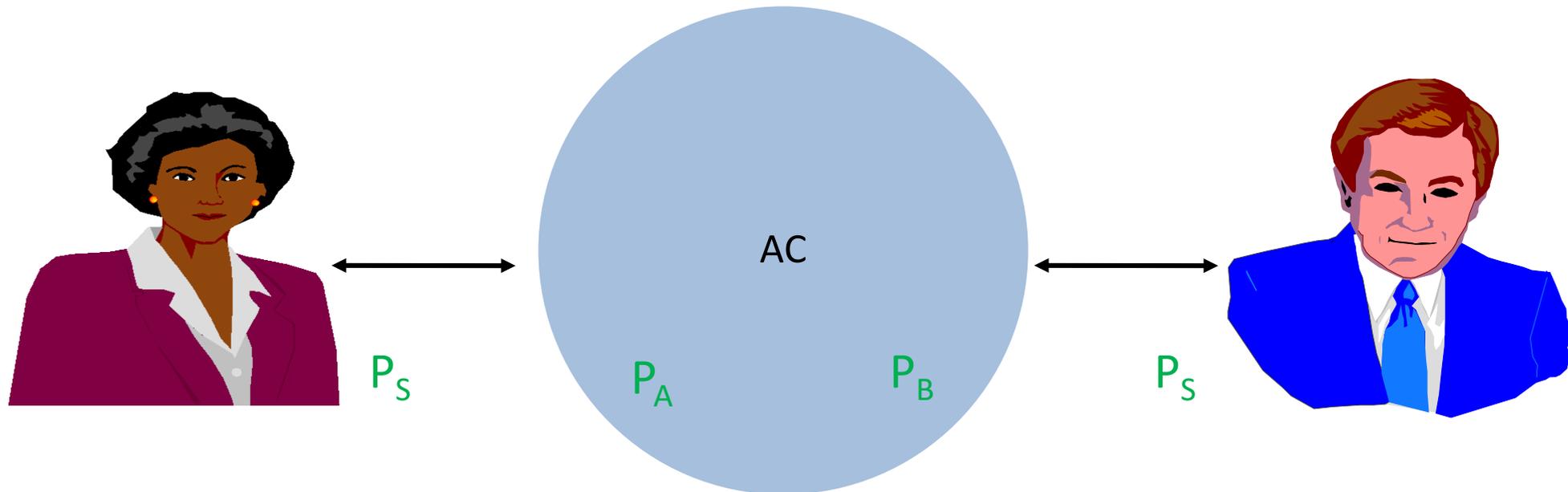


# Signature digitale par cryptographie asymétrique



# 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



## C – Sécurité des Communications

- ▶ *I – Sécurité de l'Information*
  
- ▶ **C – Sécurité des Communications**
  - **Authentification des utilisateurs**
  - **Identification des utilisateurs**
  
- ▶ *C – Sécurité du Calcul*

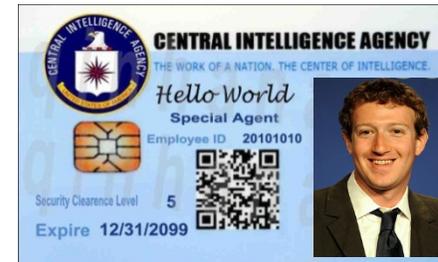
# Authentification à distance

► Identification & authentification  
= =  
Désignation reconnaissance

↓  
"userid"

► Trois possibilités: sur base de

- Quelque chose que l'utilisateur **connait**: 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 **rentrés** dans le terminal qui les capture
  - ⇒ **Supprimer leur affichage** à l'écran
  - ⇒ Se méfier **des maliciens** espions (key-loggers – risque majeur)
  - ⇒ Se méfier **des caméras**
  - ⇒ **cacher leur saisie** au clavier
- ▶ Les mots de passe doivent être **transmis à** et **stockés dans** l'ordinateur qui les vérifie => **cryptés**
  - ⇒ **"salés" + hachés** avant transmission
  - ⇒ **"salés" + hachés** dans une liste de mots de passe **à accès restreint**
- ▶ Les mots de passe ne doivent **JAMAIS** être écrits nulle part  
=> **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	corvette	porsche	player	james	angels	firebird	flyers	fred	scott	prince	suckit	ladies	asdfgh	rosebud	danielle	calvin	girl									
12345678	pepper	cheese	chelsea	morgan	brandon	dauid	united	porn	3434x	asdf	amateur	buddy	giants	toyota	great	4341	surfer	parker								
1234	1111	matthew	black	starwars	fender	whatever	booty	travis	cool	4128	samson	qwerty	young	blonde	hotdog	cooper	runner	kelly	time							
12345	290'731 instances sur 32M de mots de passe analysés!	diamond	boomer	anthony	butthead	jason	donald	marlboro	star	testing	sydney	women	voodoo	magnum	stupid	5555	juice	shit	eagle	abgrtyu						
dragon	qwerty	696969	tigger	summer	ginger	654341	gins	cricken	golf	cumshot	bronco	internet	shannon	erotic	brazil	hentai	77777	frank	midnight	erotic	brazil	shit	eagle	abgrtyu		
mustang	robert	heather	blowjob	computer	booboo	mave	captain	bond007	boston	penis	action	murphy	monica	tedskins	987654	stupid	5555	juice	frank	midnight	erotic	brazil	shit	eagle	abgrtyu	
letmein	access	hammer	nicole	amanda	coffee	go	bigdick	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	
baseball	love	yankees	sparky	wizard	34343	joseph	chester	smokey	xavier	gator	victor	white	jeremy	brian	0	arsenal	squirt	stars	mark	chevy	access14	stars	apple	alexis	aaaa	
master	buster	joshua	yellow	34343	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	hannah	
football	soccer	biteme	secret	ph	re	steven	gator	victor	white	jeremy	brian	0	arsenal	squirt	stars	apple	alexis	aaaa	mark	chevy	access14	stars	apple	alexis	aaaa	
shadow	hockey	enter	dick	mickey	peanut	666666	viking	ang	tucker	topgun	11111111	er	mark	chevy	access14	stars	apple	alexis	aaaa	mark	chevy	access14	stars	apple	alexis	aaaa
monkey	killer	ashley	falcon	bailey	john	willie	snoop	access	bigtits	bill	nathan	startrek	winston	wolf	apple	alexis	aaaa	mark	chevy	access14	stars	apple	alexis	aaaa	peaches	
abc123	george	thunder	taylor	knight	johnny	welcome	thx1138	bitches	cry	raiders	sierra	warrior	nipple	alexis	aaaa	mark	chevy	access14	stars	apple	alexis	aaaa	peaches	peaches		
pass	sexy	cowboy	111111	iceman	gandalf	chris	qazwsx	green	peter	steve	leather	sammy	iloveyou	aaaa	mark	chevy	access14	stars	apple	alexis	aaaa	peaches	peaches			
fuckme	andrew	silver	131313	tigers	spanky	panther	winner	badboy	doggy	russies	forever	234343	alex	h	peaches	peaches	peaches	peaches	peaches	peaches	peaches	peaches	peaches	peaches	peaches	
6969	charlie	richard	123123	purple	winter	yamaha	samantha	debbie	angela	vinor	jasmine	rainbow	skippy	phantom	peaches	peaches	peaches	peaches	peaches	peaches	peaches	peaches	peaches	peaches	peaches	
jordan	harley	asshole	orange	hello	horny	compaq	banana	imma	horney	lakers	nipples	legend	kevin	112234	marvin	billy	6666	peaches	peaches	peaches	peaches	peaches	peaches	peaches	peaches	
ranger	fuckyou	merlin	scooter	dakota	carlos	driver	flower	booger	bubba	rachel	ou812	power	movie	matt	arthur	blondes	6666	peaches	peaches	peaches	peaches	peaches	peaches	peaches	peaches	
iwantu	dallas	michelle	please	aaaaaa	tennis	marine	jack	1212	2112	slayer	oliver	sophie	victoria	success	qwertyui	cream	enjoy	albert	peaches	peaches	peaches	peaches	peaches	peaches	peaches	

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

ncc1701

le titre du 1er film de George Lucas

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

thx1138

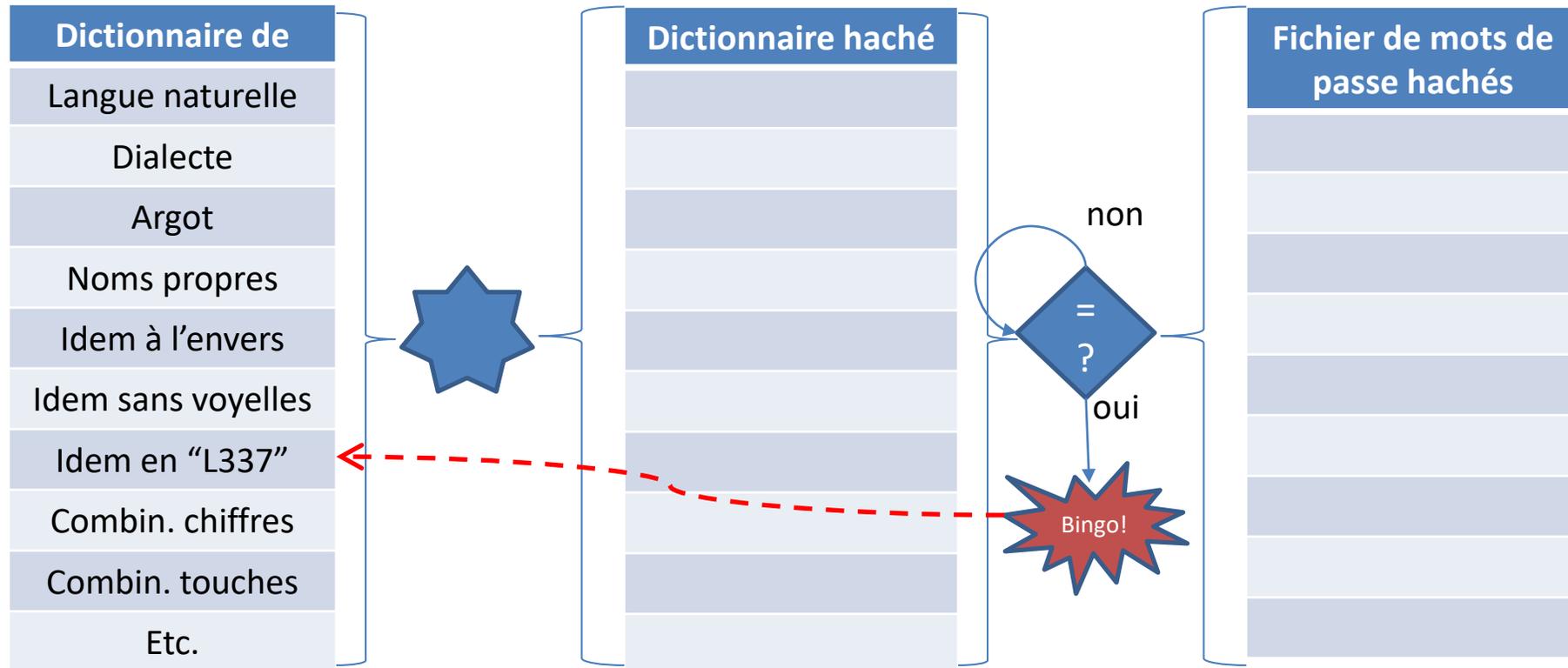
le titre d'un album de Van Halen en 1988

qazwsx

8675309

ou812

# 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 un mot de passe

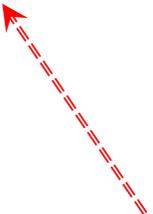
- Les mots de passe doivent avoir une longueur suffisante pour résister aux devinettes

Risque **R** = durée de vie **D** x fréquence des attaques **F** / taille de l'alphabet **T** (taille du mot de passe **M**)

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

8 > log ( 100 J x 100 / J / 10<sup>-9</sup> ) / log 62

entropie maximale



⇒ **Changer de mot de passe régulièrement** (chaque année ou même chaque trimestre)

⇒ **Utiliser des alphabets assez vastes** – 26 majuscules + 26 minuscules + 10 chiffres + ? Signes

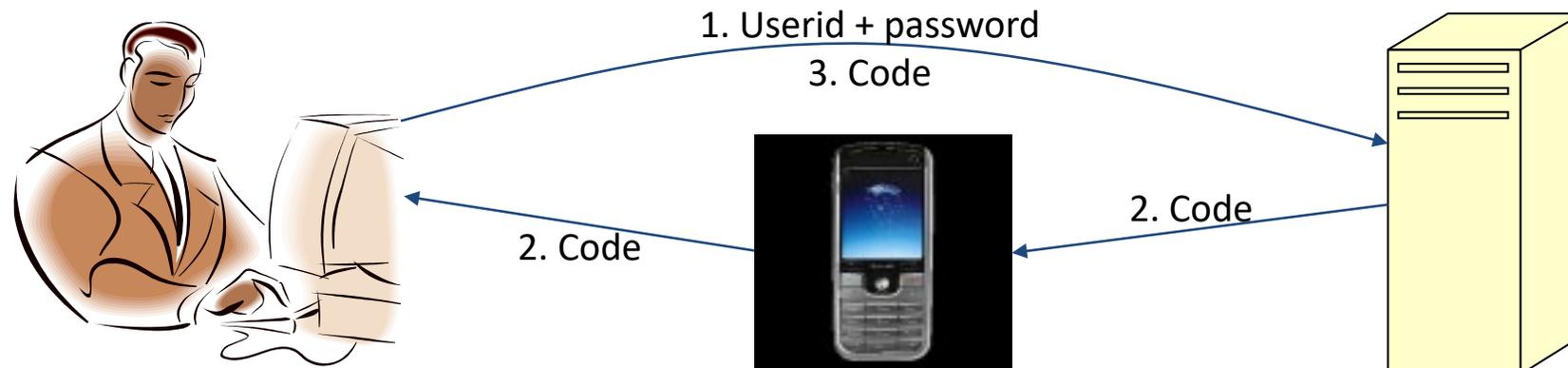
⇒ **Limiter la fréquence des attaques** pour déjouer des attaques programmées

⇒ **Ne jamais réutiliser le même mot de passe** sur plusieurs systèmes (“password sloth”)

# 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



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

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

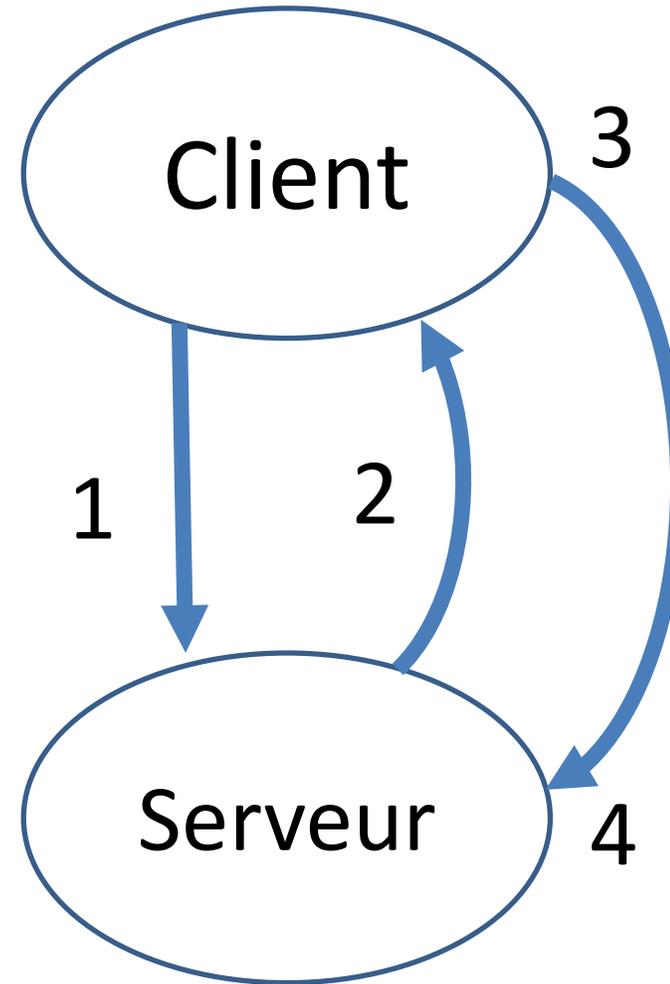
## Authentification bi-directionnelle

- ▶ Toutes les techniques vues jusqu'ici n'offrent qu'une authentification **UNIDIRECTIONNELLE**
- ▶ Ceci représente une carence et un risque MAJEUR (“phishing / pharming”)
- ▶ Sans cryptographie, le premier partenaire qui s'identifie à l'autre doit lui révéler son mot de passe
- ▶ La solution est une identification cryptographique **bi-directionnelle**
  - C'est exactement ainsi que fonctionnent les protocoles HTTPS / SSL / TLS (icône  )



- 1) Demande d'authentification + liste des cryptosystèmes supportés
- 2) Certificat du serveur avec sa **clef publique** signée par une autorité de certification
- 3) Vérification du certificat
  - création d'une **clef secrète** chiffrée avec la **clef publique** du serveur
- 4) La **clef secrète** est déchiffrée avec la **clef privée** du serveur

La suite des communications s'effectue avec la **clef secrète** (cryptage symétrique)



## T – Sécurité du Traitement informatique et de ses équipements

- ▶ *I – Sécurité de l'Information*
- ▶ *C – Sécurité des Communications*
- ▶ **C – Sécurité du Calcul**
  - **Autorisation**
  - **Quelques bons conseils pratiques**

# Autorisation – Politique de contrôle d'accès – Vue matricielle

Qui \ Quoi	O Logiciel	B ...	J <u>Fichier</u>	E ...	Ts Matériel
A ...					
C Logiciel					
T ...					
E <u>Utilisateur</u>					
U ...					
R Matériel					
S ...					

Permissions de l'acteur de lire / écrire / exécuter l'objet

R/W/X...

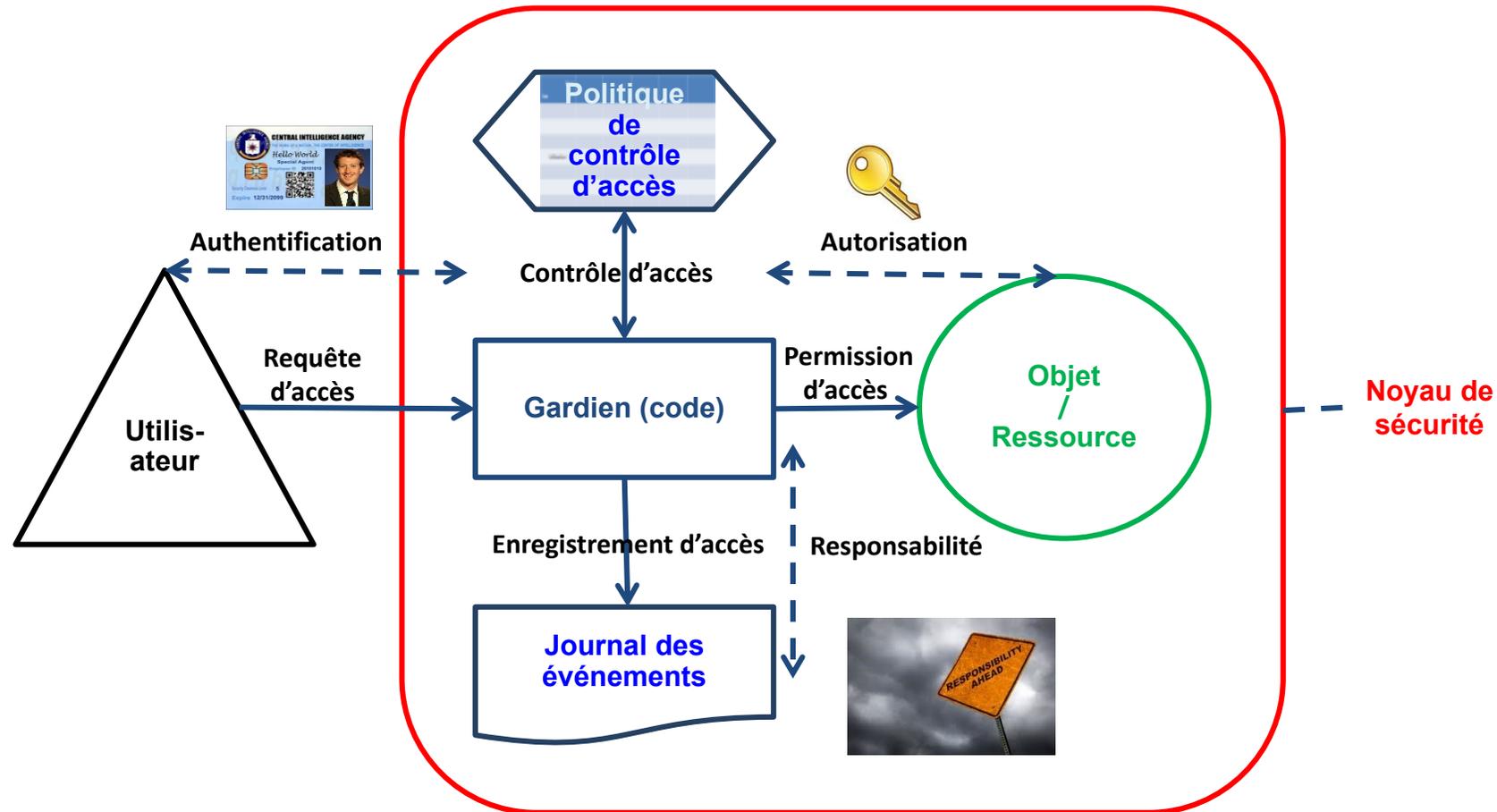




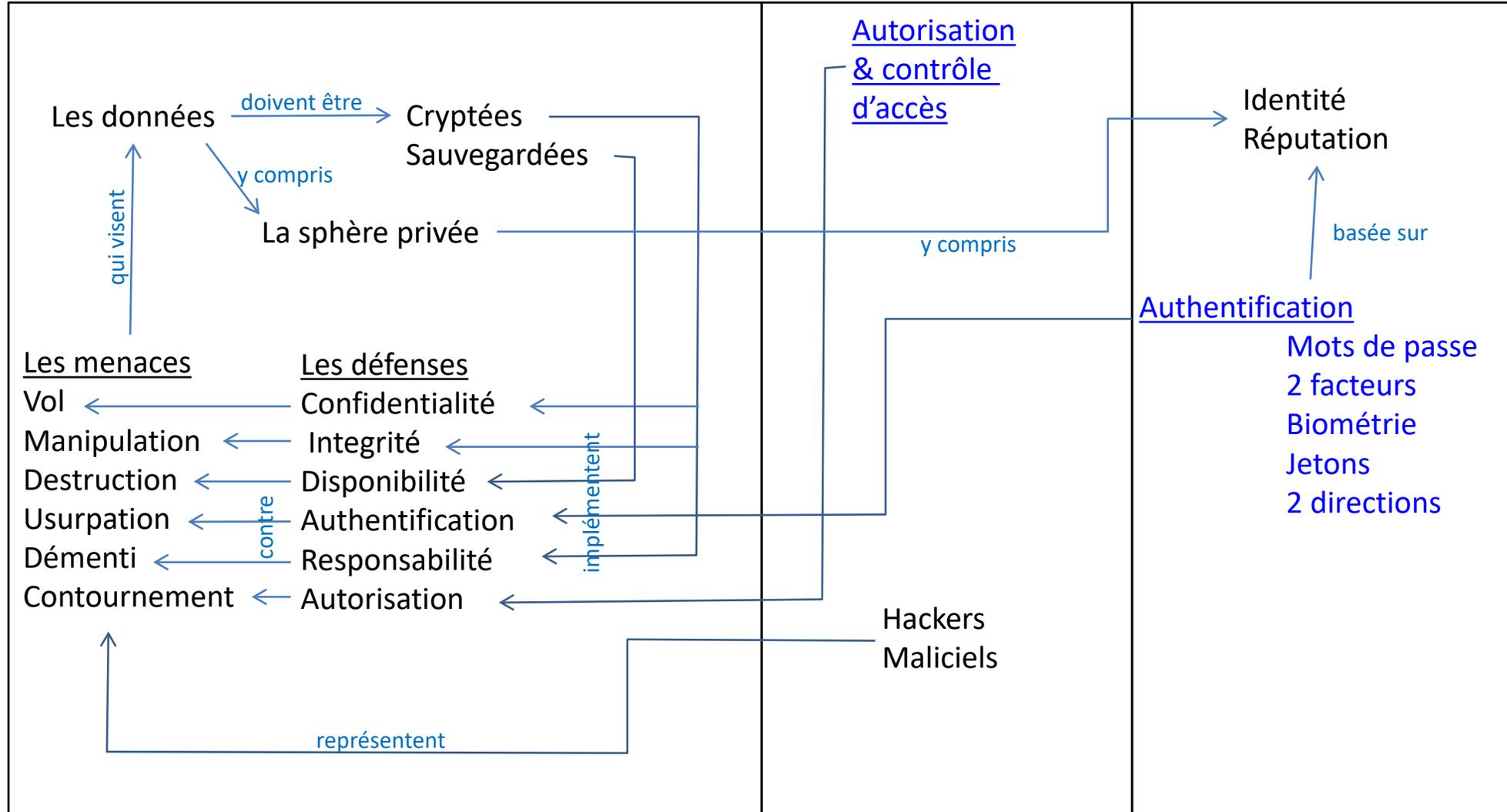
Liste de contrôle d'accès associée à l'objet

# 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**



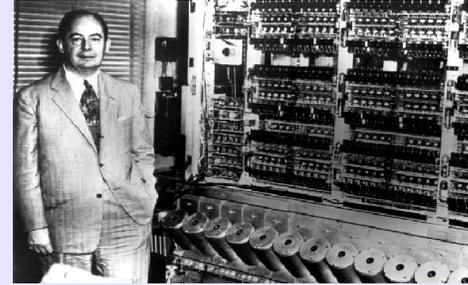
# Synthèse des enjeux



## 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





## Information, Calcul et Communication

Fin