La sécurité informatique

Chaire Informatique et sciences numériques
Collège de France, 10 mars 2011

Les drones américains piratés pour 26 dollars

LEMONDE.FR | 17.12.09 | 18h28 • Mis à jour le 17.12.09 | 18h34

EDF Should Face Greenpeace Computer-Hacking Trial, French Prosecutor Says

By Heather Smith - Sep 6, 2010

Bloomberg

Hackean el Twitter de los astronautas

25/07/10

Clarín.com Internet

WSJ.com

EUROPE TECHNOLOGY | JULY 22, 2010

Virus Attacks Siemens Plant-Control Systems

Les Etats-Unis veulent renforcer leurs capacités d'espionnage du Web

LEMONDE.FR | 27.09.10 | 15h59 • Mis à jour le 27.09.10 | 16h33

Citigroup aurait perdu des dizaines de millions de dollars dans une cyberattaque

LEMONDE.FR avec Reuters | 22.12.09 | 10h16 • Mis à jour le 22.12.09 | 10h35

Wake up to £17bn cybercrime, business told

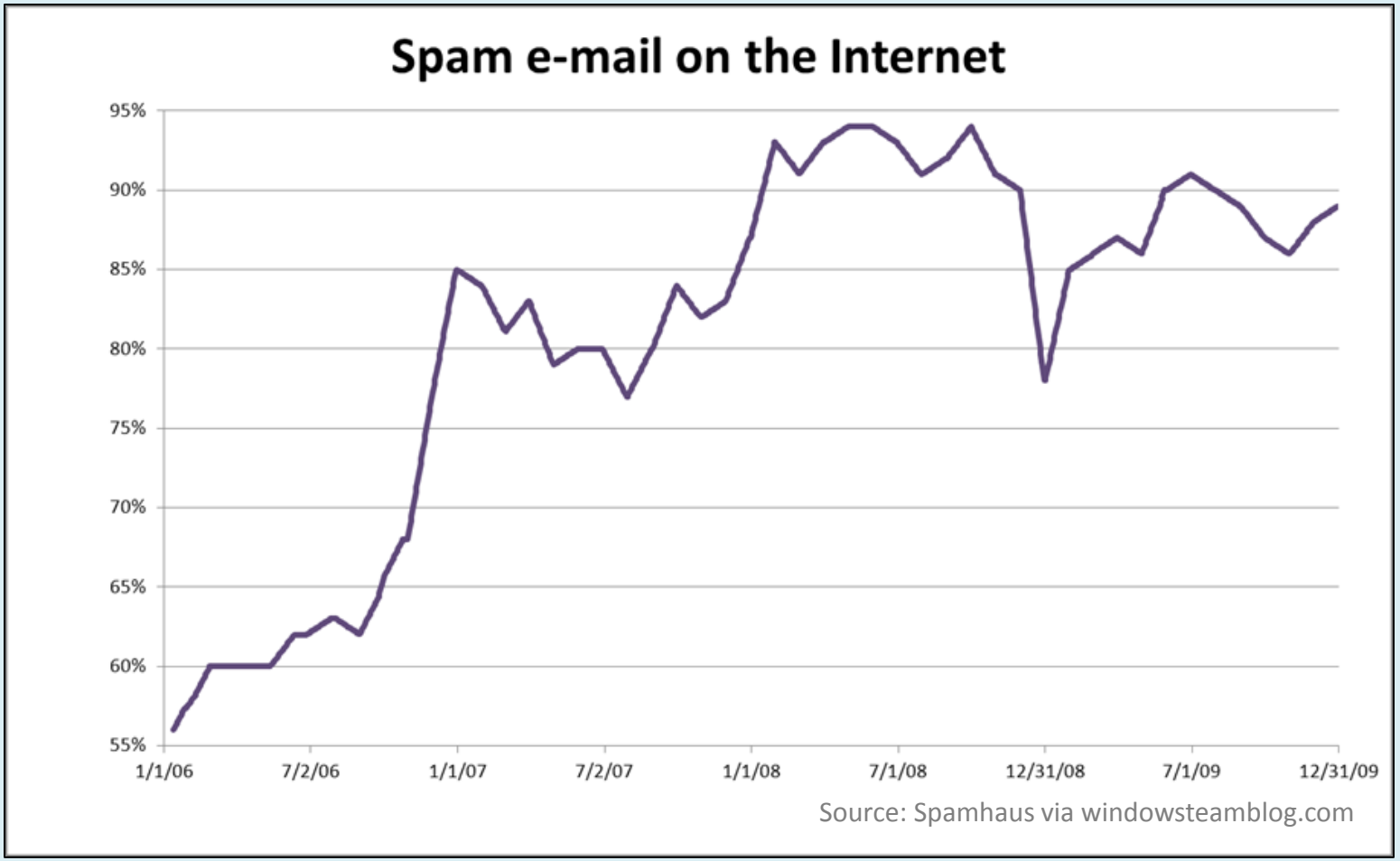
By James Boxell and Mary Watkins

Published: February 17 2011 13:36 | Last updated: February 17 2011 22:10

FT.com FINANCIAL TIMES

- *Un exemple: du spam et des botnets à l'arithmétique modulaire*
- *Contenu du cours*
- *Qu'entend-on par sécurité ?*
- *Alice et Bob au pays du pi calcul*
- *Difficulté du savoir*

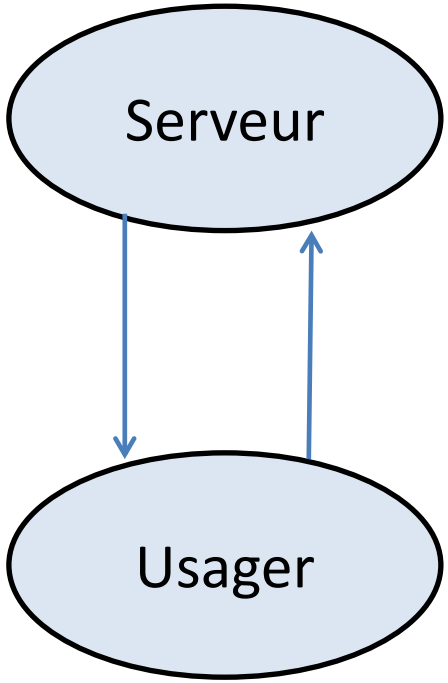
Du spam et des botnets
à l'arithmétique modulaire



Le spam s'en va et puis revient

LEMONDE.FR | 04.03.11 | 18h49 • Mis à jour le 04.03.11 | 18h49

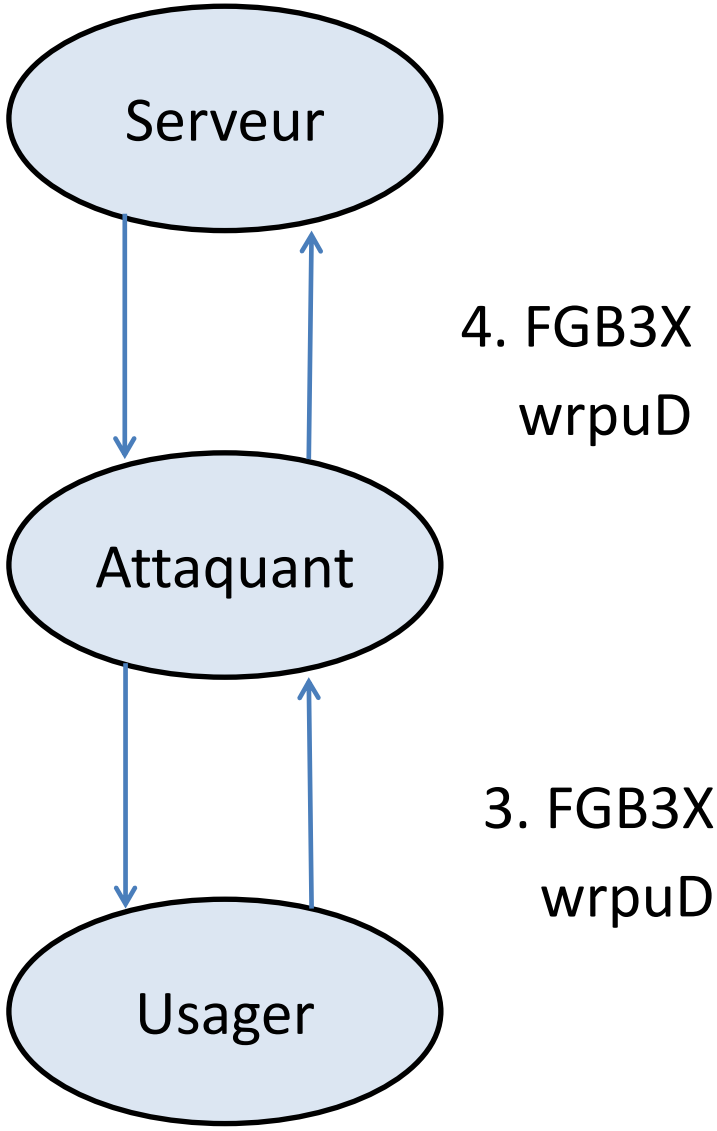
1. Pour accéder au service, veuillez bien transcrire

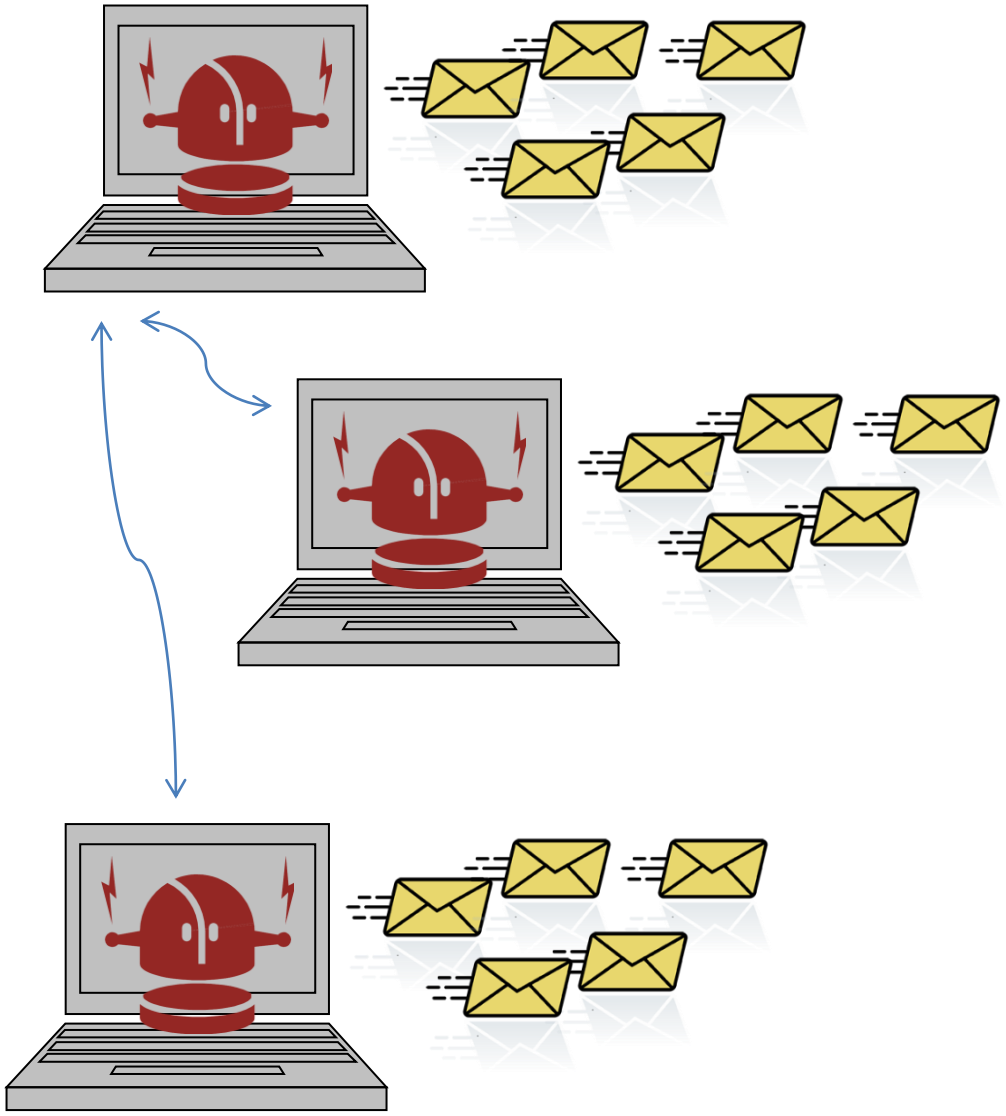


2. FGB3X
wrpuD

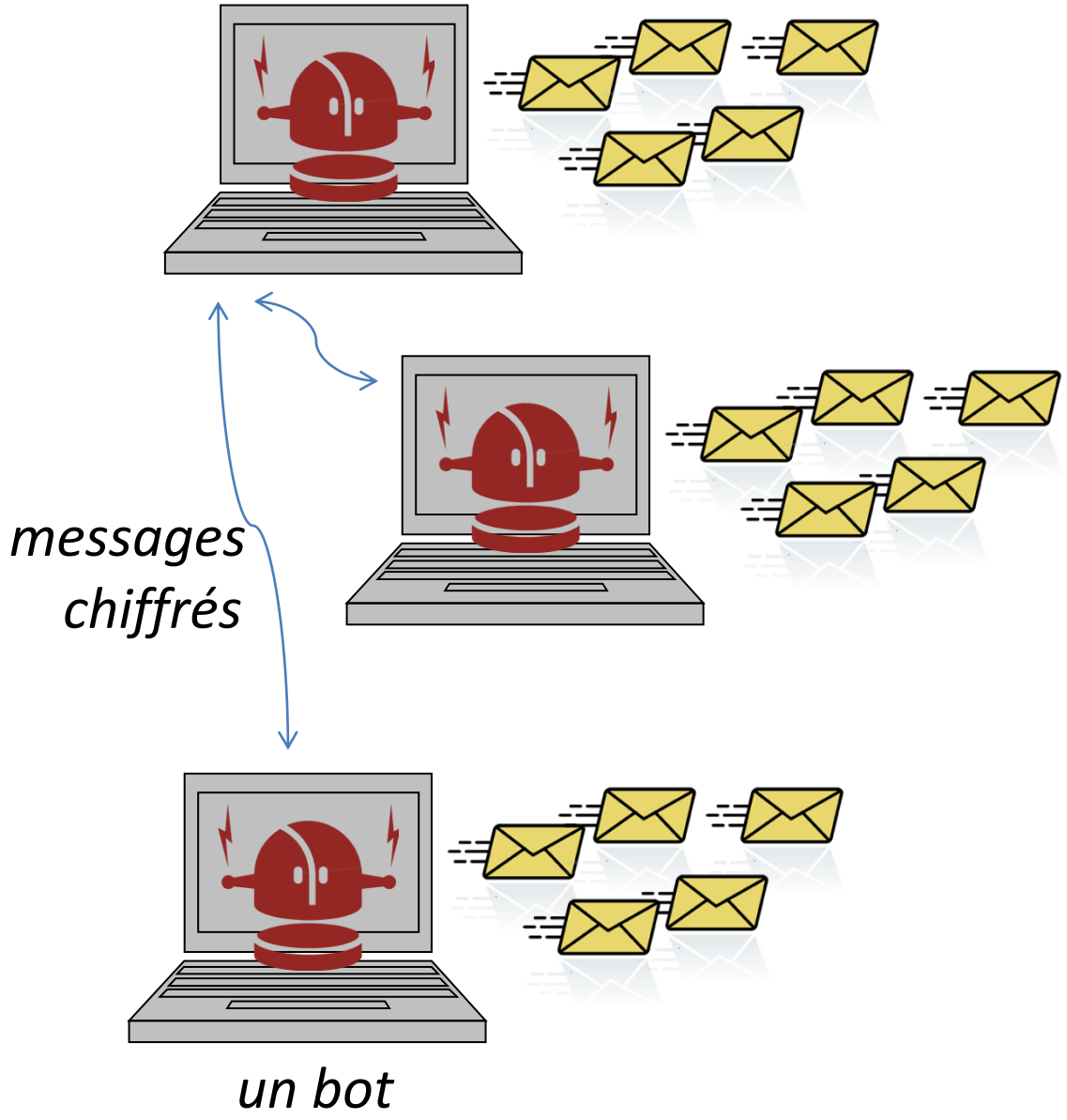
1. Pour accéder au service,
veuillez bien transcrire

2. Pour jouer,
veuillez bien transcrire

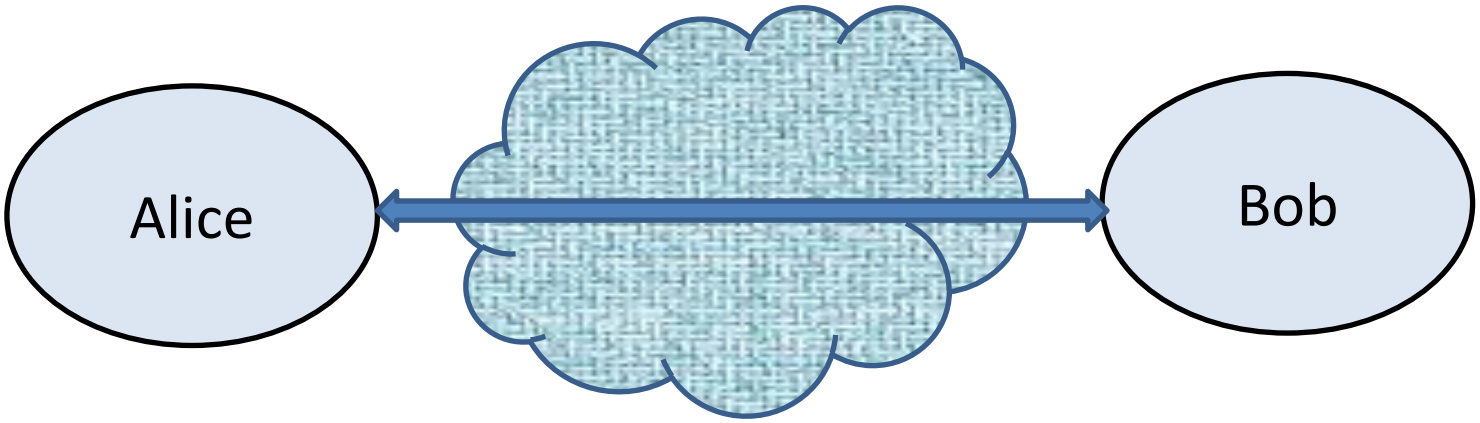




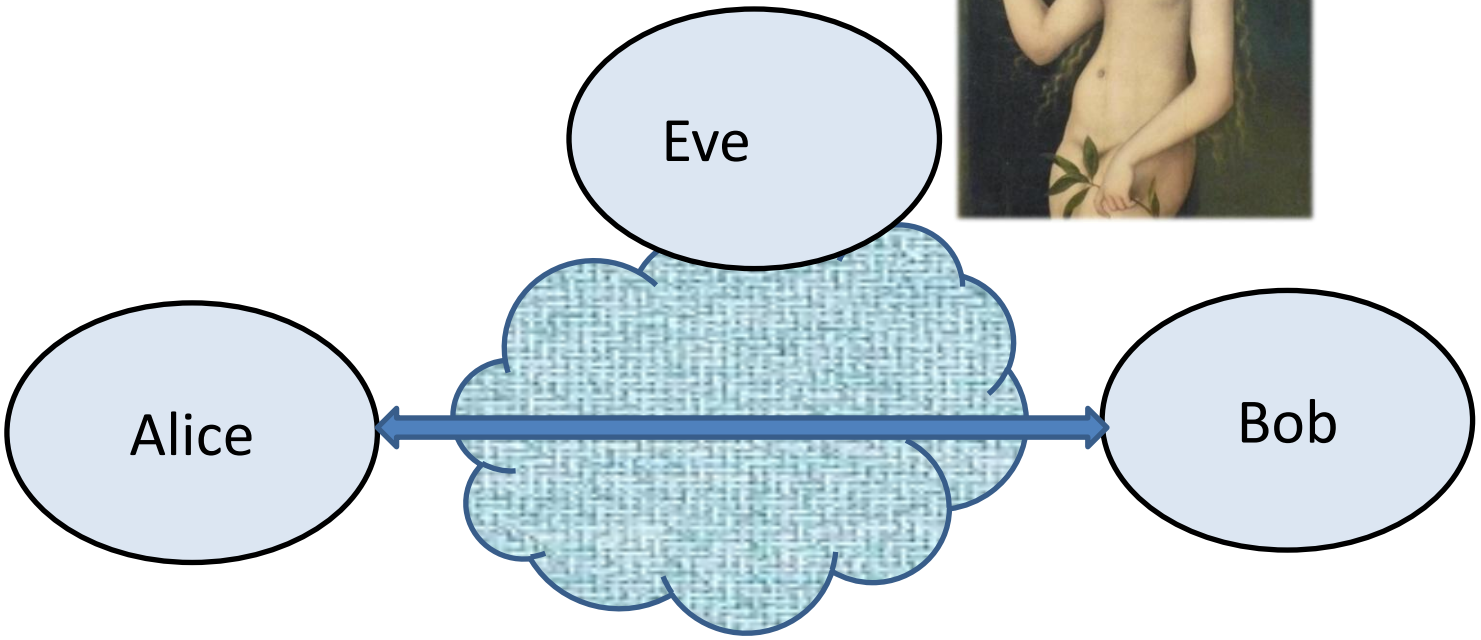
un bot


messages
chiffrés
un bot

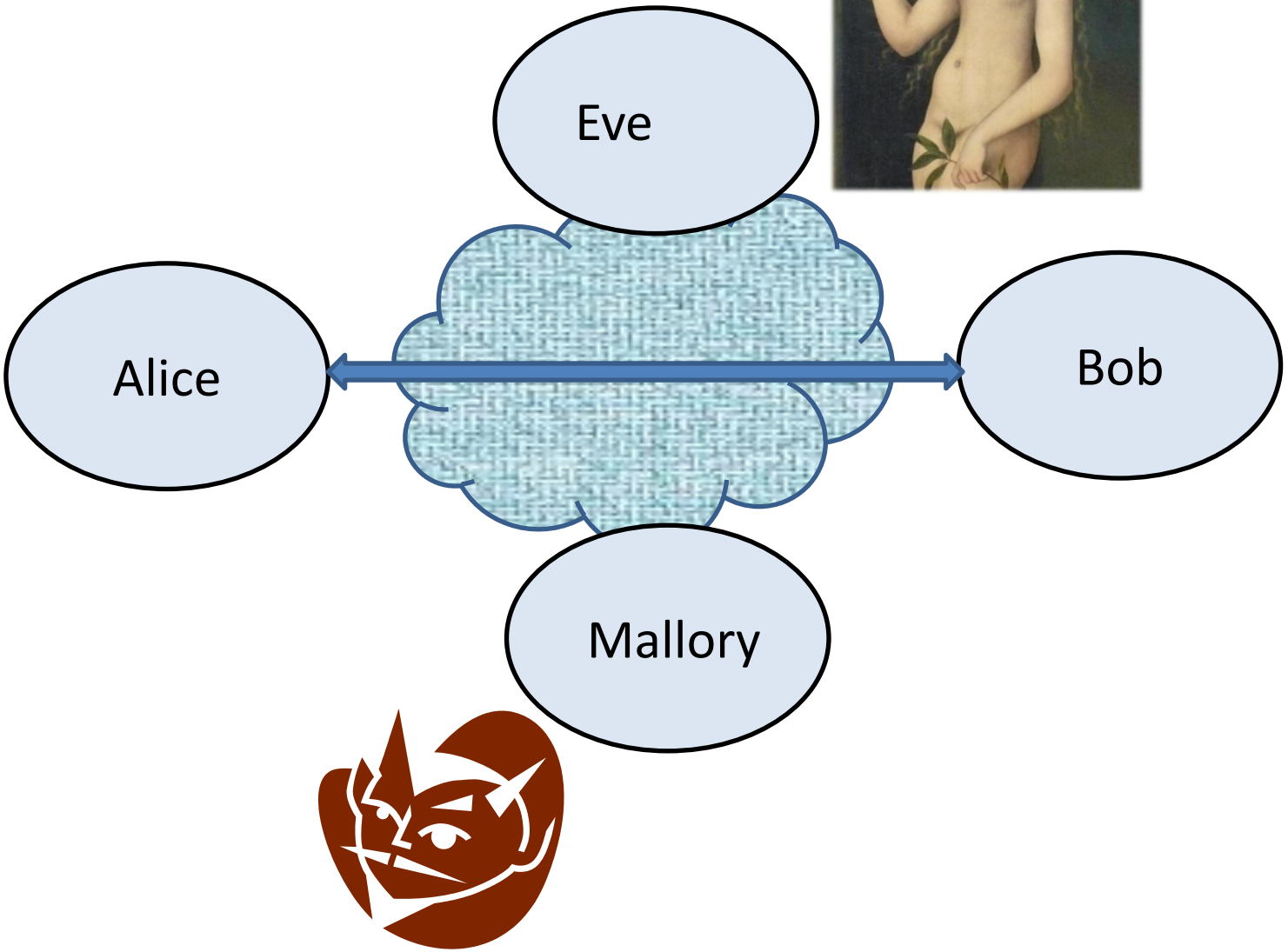
Personnages



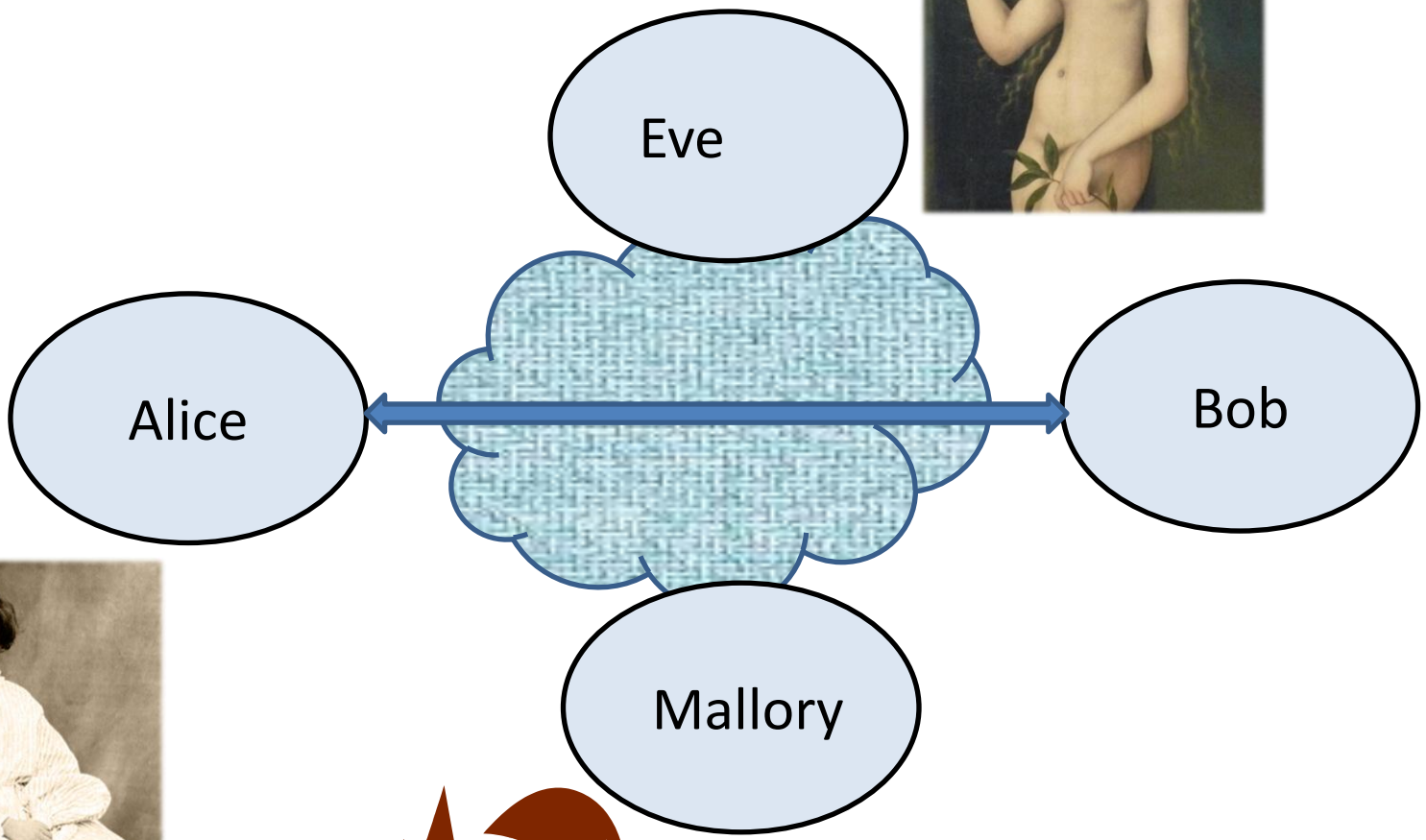
Personnages



Personnages



Personnages



Personnages

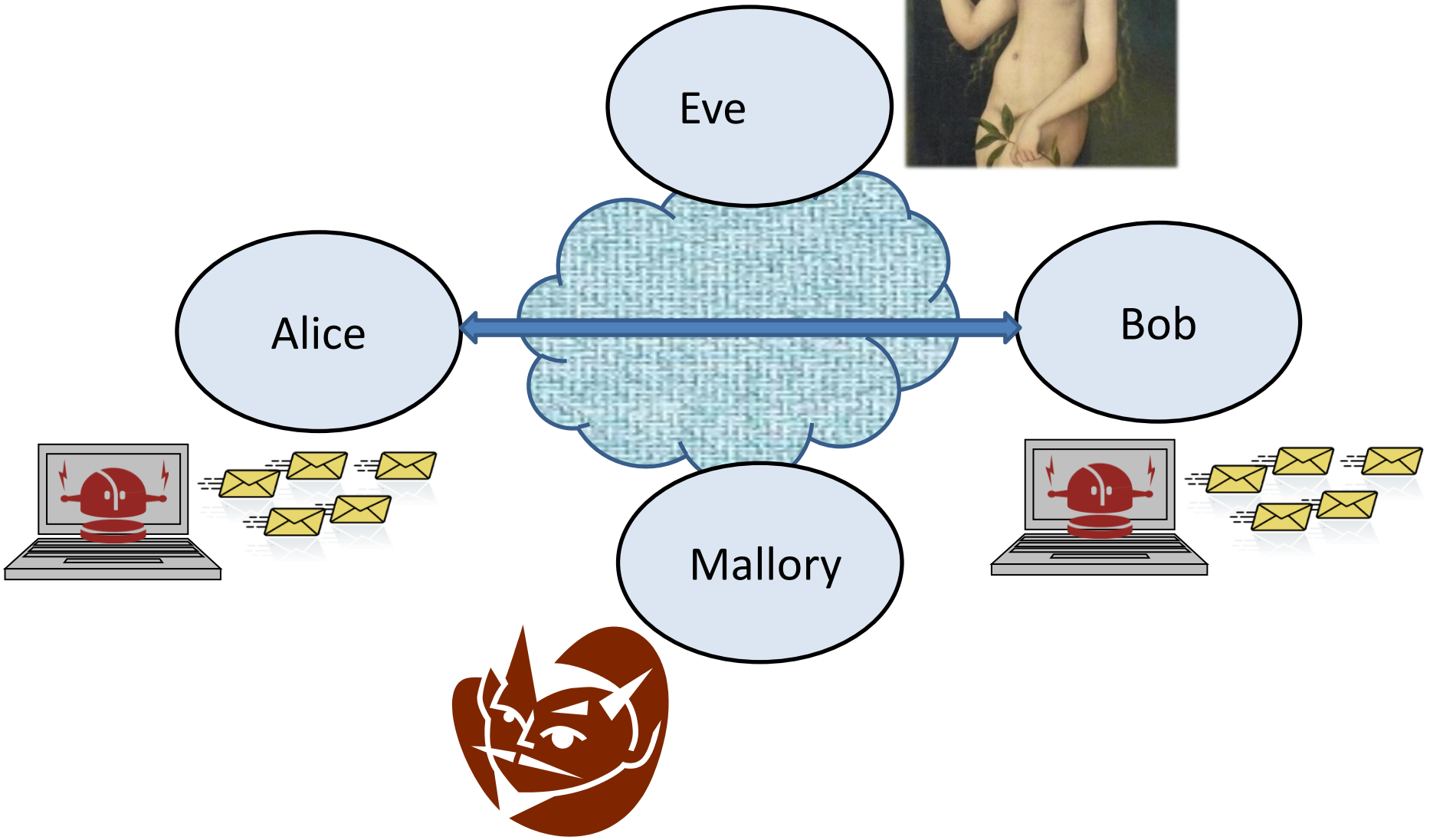
Eve

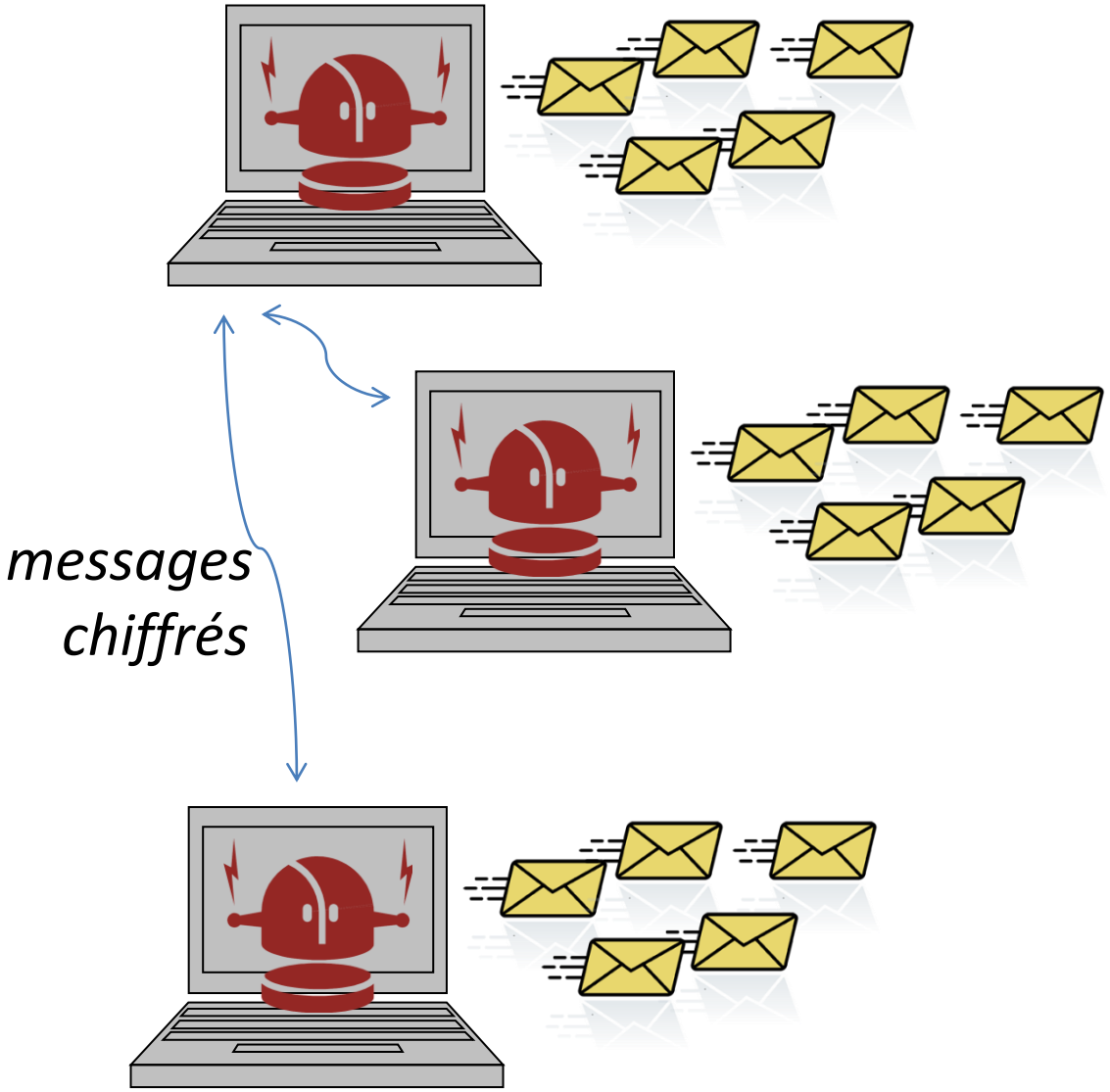
Alice

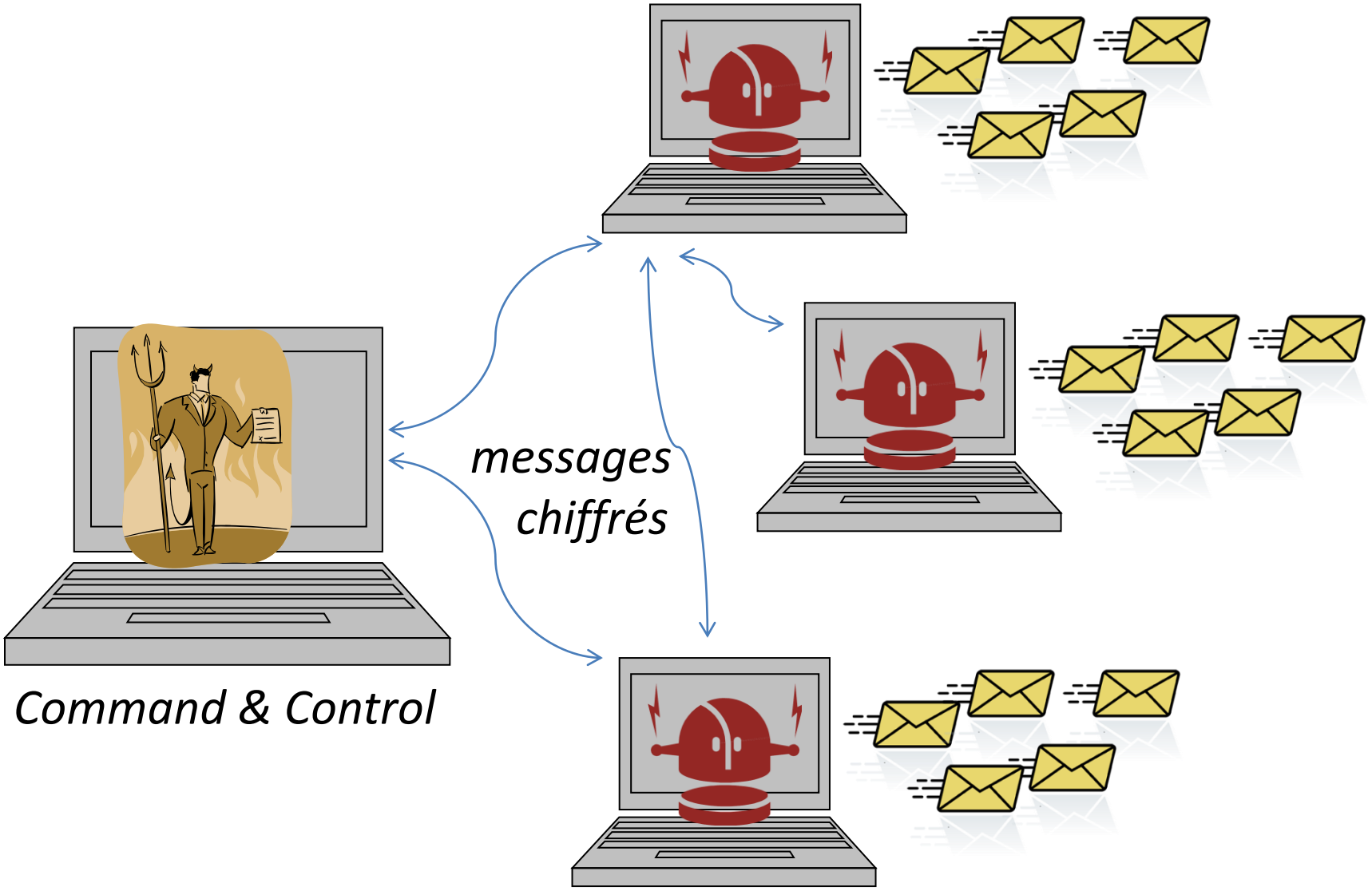
Bob

Mallory

Personnages




messages
chiffrés


messages
chiffrés
Command & Control

Exemples
[John et al., 2009]

Nom du botnet	Communication avec le Command & Control	Découverte du Command & Control	Messages envoyés par minute par chaque bot
Grum	HTTP chiffré	adresse IP fixe	344
Kraken	HTTP chiffré	noms DNS	331
Pushdo	HTTP chiffré	adresses IP fixes	289
Rustock	HTTP chiffré	adresse IP fixe	33
MegaD	protocole ad hoc	nom DNS fixe	1638
Srizbi	HTTP	adresses IP fixes	1848
Storm	TCP (comprimé)	P2P (*Overnet*)	20

Ces données ont été obtenues avec ***Botlab***, un des outils pour analyser les botnets.

New | Reply Reply all Forward | Delete Junk Sweep ▾ Mark as ▾ Move to ▾ |

aveux

Back to messages |

xyz xyz Add to contacts
To jemappellepatrickmaisonditbob@hotmail.com

10:53 AM
Reply ▾

From: **xyz xyz** (admiratrice2011@hotmail.com)
Sent: Mon 10/04/10 10:53 AM
To: jemappellepatrickmaisonditbob@hotmail.com
1 attachment
ILoveYou.jpg (14.0 KB)

Attachments, pictures and links in this message have been blocked for your safety.
Show content | Always show content from this sender

New | Reply Reply all Forward | Delete Junk Sweep ▾ Mark as ▾ Move to ▾ |

aveux

Back to messages |

xyz xyz Add to contacts
To jemappellepatrickmaisonditbob@hotmail.com

10:53 AM
Reply ▾

From: **xyz xyz** (admiratrice2011@hotmail.com)
Sent: Mon 10/04/10 10:53 AM
To: jemappellepatrickmaisonditbob@hotmail.com
1 attachment
ILoveYou.jpg (14.0 KB)

Attachments, pictures and links in this message have been blocked for your safety.
Show content | Always show content from this sender

New | Reply Reply all Forward | Delete Junk Sweep ▾ Mark as ▾ Move to ▾ |

aveux

Back to messages |

xyz xyz Add to contacts
To jemappellepatrickmaisonditbob@hotmail.com

10:53 AM
Reply ▾

From: **xyz xyz** (admiratrice2011@hotmail.com)
Sent: Mon 10/04/10 10:53 AM
To: jemappellepatrickmaisonditbob@hotmail.com

Always show content from this sender

1 attachment | Hotmail Active View

View slide show (1)

New | Reply Reply all Forward | Delete Junk Sweep ▾ Mark as ▾ Move to ▾ |

aveux

Back to messages |

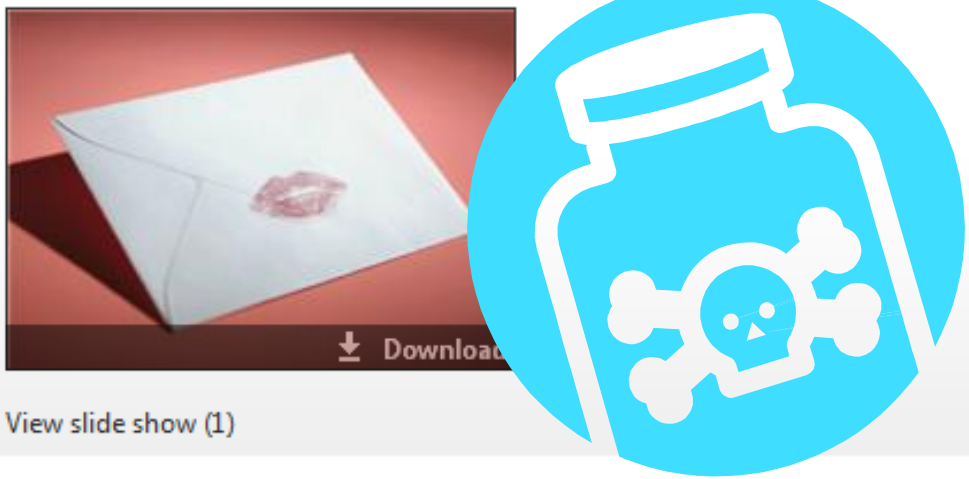
xyz xyz Add to contacts
To jemappellepatrickmaisonditbob@hotmail.com

10:53 AM
Reply ▾

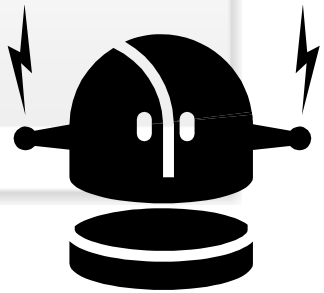
From: **xyz xyz** (admiratrice2011@hotmail.com)
Sent: Mon 10/04/10 10:53 AM
To: jemappellepatrickmaisonditbob@hotmail.com

Always show content from this sender

1 attachment | Hotmail Active View



View slide show (1)



Une étude de 32000000 mots de passe de Rockyou.com
[Imperva, 2010]

	Mot de passe	Nombre d'usagers avec le mot de passe
1	123456	290731
2	12345	79078
3	123456789	76790
4	Password	61958
5	iloveyou	51622
6	princess	35231
7	rockyou	22588
8	1234567	21726
9	12345678	20553
10	abc123	17542
11	Nicole	17168
12	Daniel	16409

New | Reply Reply all Forward | Delete Junk Sweep ▾ Mark as ▾ Move to ▾ |

aveux

Back to messages |

xyz xyz Add to contacts
To jemappellepatrickmaisonditbob@hotmail.com

10:53 AM
Reply ▾

From: **xyz xyz** (admiratrice2011@hotmail.com)
Sent: Mon 10/04/10 10:53 AM
To: jemappellepatrickmaisonditbob@hotmail.com
1 attachment
ILoveYou.jpg (14.0 KB)

Attachments, pictures and links in this message have been blocked for your safety.
Show content | Always show content from this sender

New | Reply Reply all Forward | Delete Junk Sweep ▾ Mark as ▾ Move to ▾ |

aveux

Back to messages |

xyz xyz Add to contacts
To jemappellepatrickmaisonditbob@hotmail.com

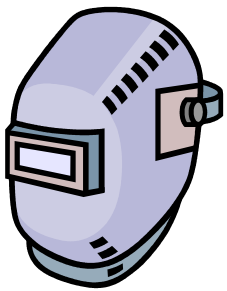
10:53 AM
Reply ▾

From: **xyz xyz** (admiratrice2011@hotmail.com)
Sent: Mon 10/04/10 10:53 AM
To: jemappellepatrickmaisonditbob@hotmail.com
1 attachment
ILoveYou.jpg (14.0 KB)

Attachments, pictures and links in this message have been blocked for your safety.
Show content | Always show content from this sender








La sécurité ne doit pas être envisagée seulement comme un problème individuel, mais aussi comme un problème social.

Egalité de devoirs : sécurité
du jeu de cartes révolutionnaires
de J. D. Dugourc, 1793-1794

Source gallica.bnf.fr / Bibliothèque nationale de France

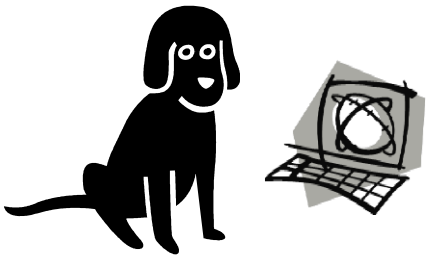
RSA (chiffrement ou signatures)

- On choisit deux nombres premiers p et q.
- Soit $n = p \times q$. On travaille modulo n.
- On choisit deux nombres e et d tels que $M^{ed} = M$ pour tout M.
- Pour chiffrer ou signer M, on calcule M^e.
- Pour retrouver M, on calcule $(M^e)^d$.
- Si p et q sont grands et secrets, il est difficile de trouver d à partir de e et n.
  (p et q étaient trop petits dans Storm.)

Contenu du cours

Cours

16 mars	Politiques de sécurité et contrôle d'accès
23 mars	Politiques de sécurité et contrôle d'accès (suite)
30 mars	Vers le contrôle des flots d'information
6 avril	La fiabilité du logiciel
27 avril	La cryptographie
4 mai	« Sur Internet, personne ne sait que vous êtes un chien », vingt ans après
11 mai	Les protocoles
18 mai	Assurance et modèles formels

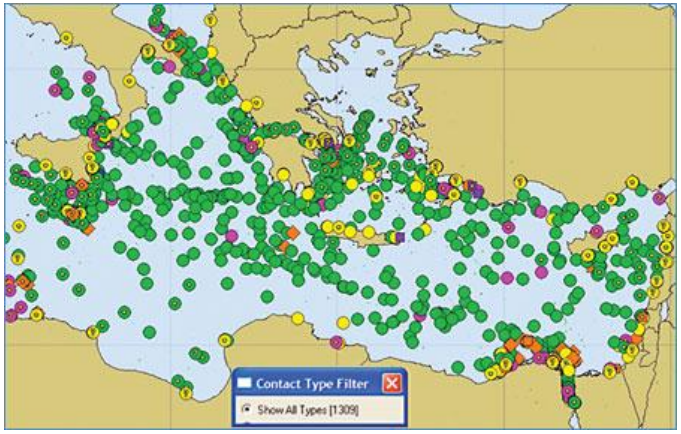


Séminaire

	**John Mitchell** (Stanford)	*16 mars*		**David Pointcheval** (CNRS)	*27 avril*
	**Ron Rivest** (MIT)	*23 mars*		**Adi Shamir** (Institut Weizmann)	*4 mai*
	**Andrew Myers** (Cornell)	*30 mars*		**Leslie Lamport** (Microsoft)	*11 mai*
	**Butler Lampson** (Microsoft)	*6 avril*		**Véronique Cortier** (CNRS)	*18 mai*

Qu'entend-on par sécurité ?

La sécurité informatique ressemble à la sécurité dans d'autres cadres.



Aux traitres, aux Fripons, que son exemple apprenne ;
que tôt ou tard le Crime est atteint par la peine.

Le veritable Portrait tiré d'apres nature sur la place du Palais Royal, d'Emanuel Jean de la Coste, condamné par Jugement Souverain de Mr. le Lieutenant Gl de Police, du 28 aoust 1760. au Carcan pendant 3. jours ala marque, et aux Galeres aperpetuité.

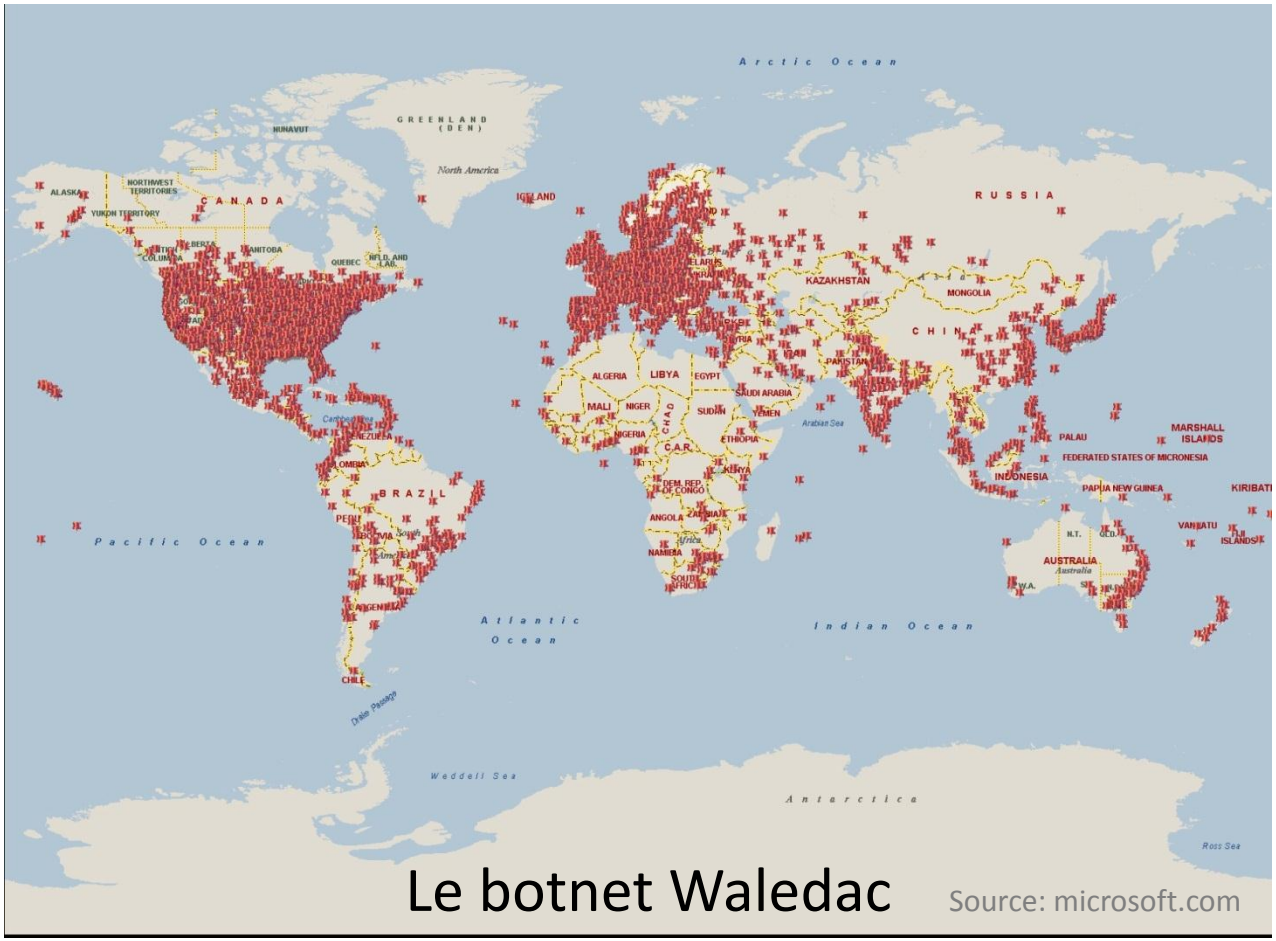
avec Permission

G 16016

8967

d.N.2.

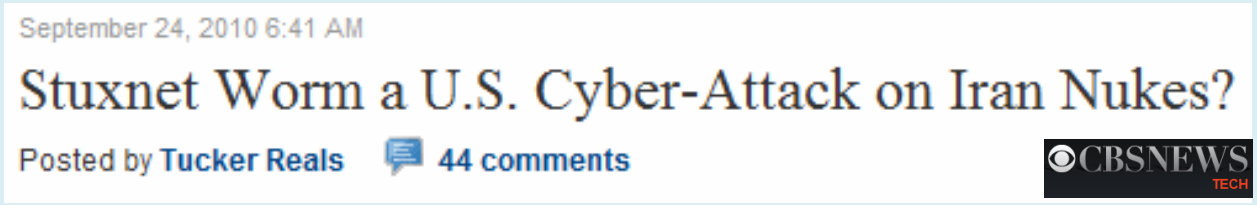
Pourtant, la sécurité informatique a des caractéristiques spécifiques.

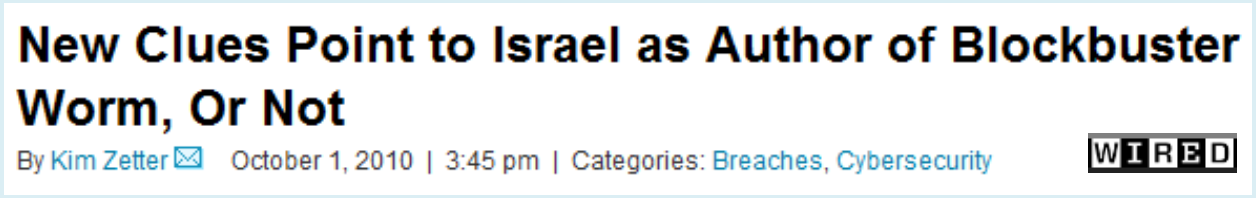


Le botnet Waledac Source: microsoft.com

Les attaques peuvent être montées de loin.
Elles sont facilement automatisées, et peuvent toucher rapidement des cibles partout dans le monde, en affectant tous les secteurs de nos activités.

Les attaquants restent anonymes assez facilement. Quelquefois même l'origine géographique d'une attaque est difficile à établir.





Il suffit de penser que l'acquisition d'un bien ou la fuite d'un mal est possible, pour être incité à la désirer. Mais quand on considère, outre cela, s'il y a beaucoup ou peu d'apparence qu'on obtienne ce qu'on désire, ce qui nous représente qu'il y en a beaucoup, excite en nous l'espérance, et ce qui nous représente qu'il y en a peu, excite la crainte, dont la jalousie est une espèce. Lorsque l'espérance est extrême, elle change de nature et se nomme sécurité ou assurance.

Descartes

Any information that you put into a computer is public information.

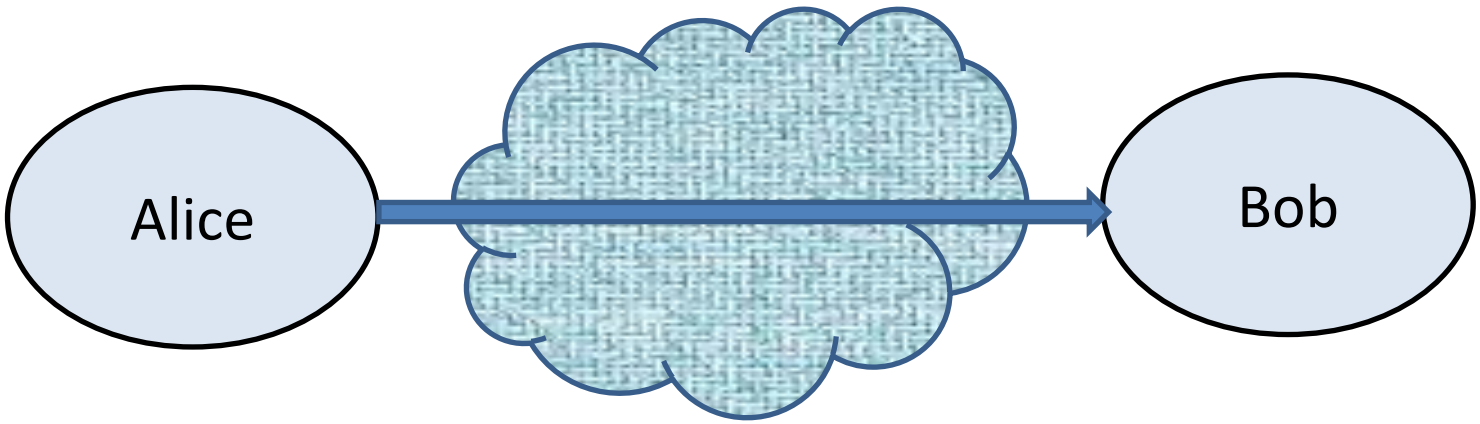
Thacker

Propriétés

- *Intégrité* (ou *authenticité*).
- *Secret* (ou *confidentialité*).
- *Disponibilité*.

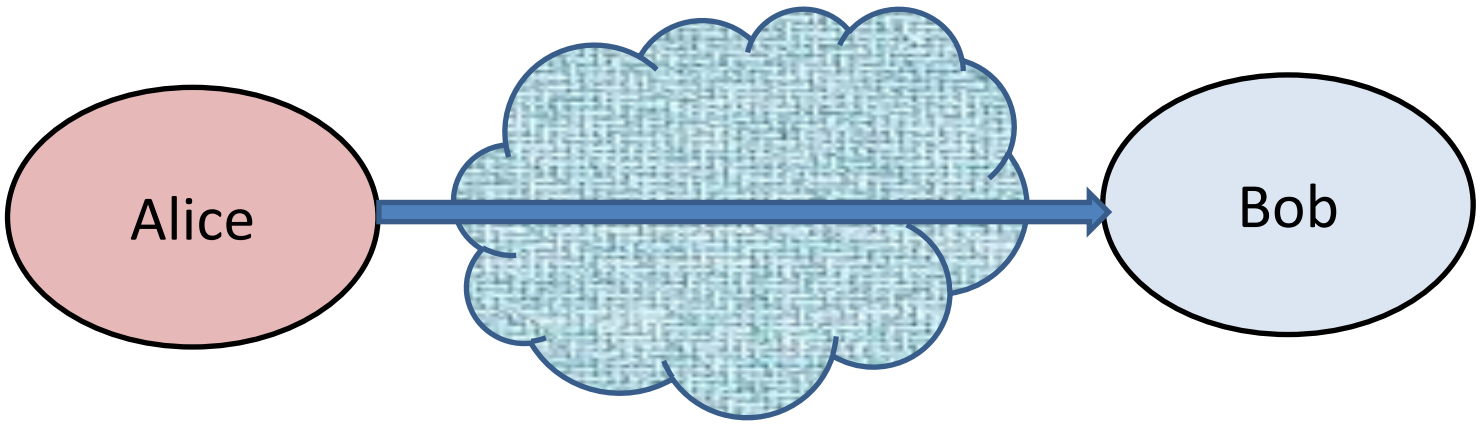
Propriétés

- *Intégrité* (ou *authenticité*).
- *Secret* (ou *confidentialité*).
- *Disponibilité*.



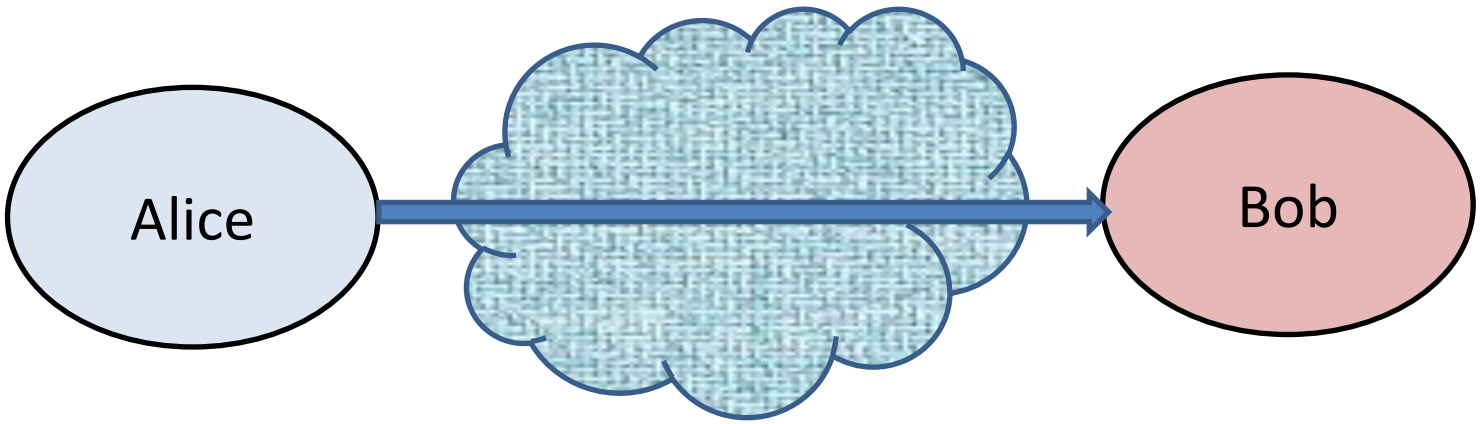
Propriétés

- *Intégrité* (ou *authenticité*).
- *Secret* (ou *confidentialité*).
- *Disponibilité*.



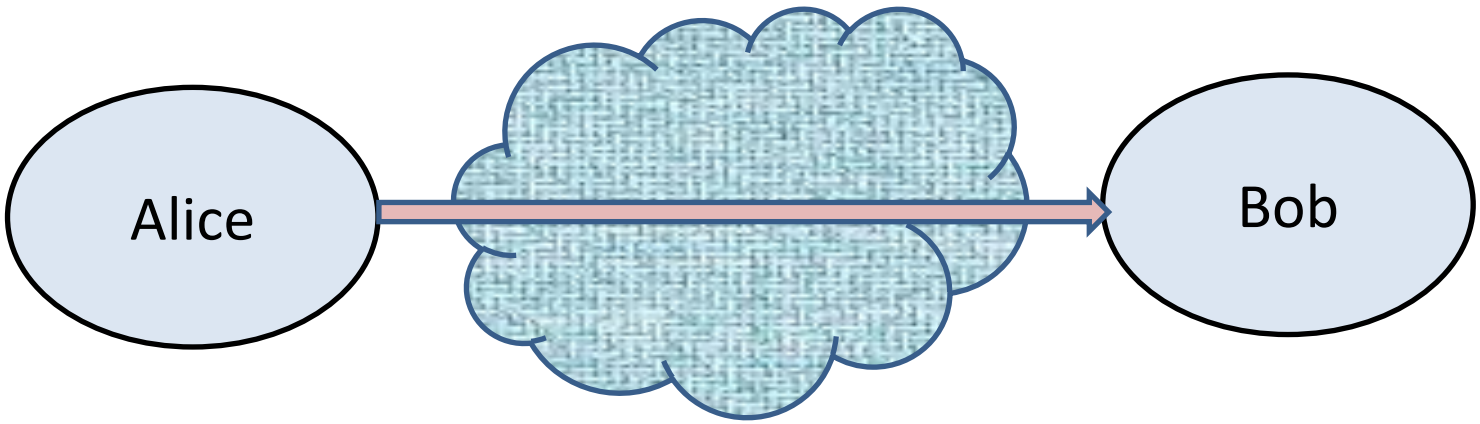
Propriétés

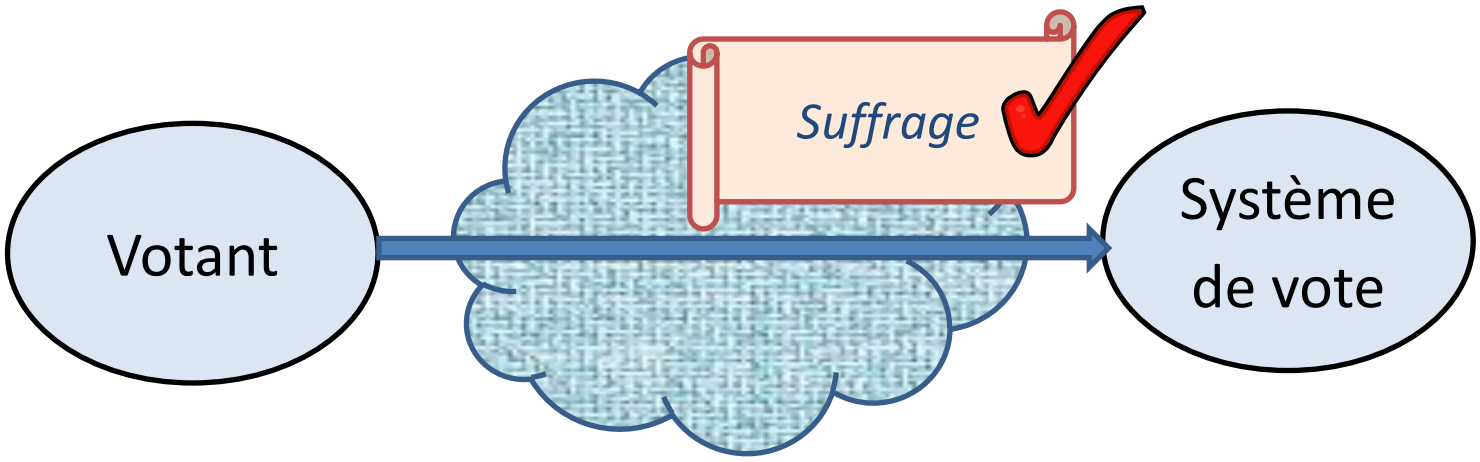
- *Intégrité* (ou *authenticité*).
- *Secret* (ou *confidentialité*).
- *Disponibilité*.

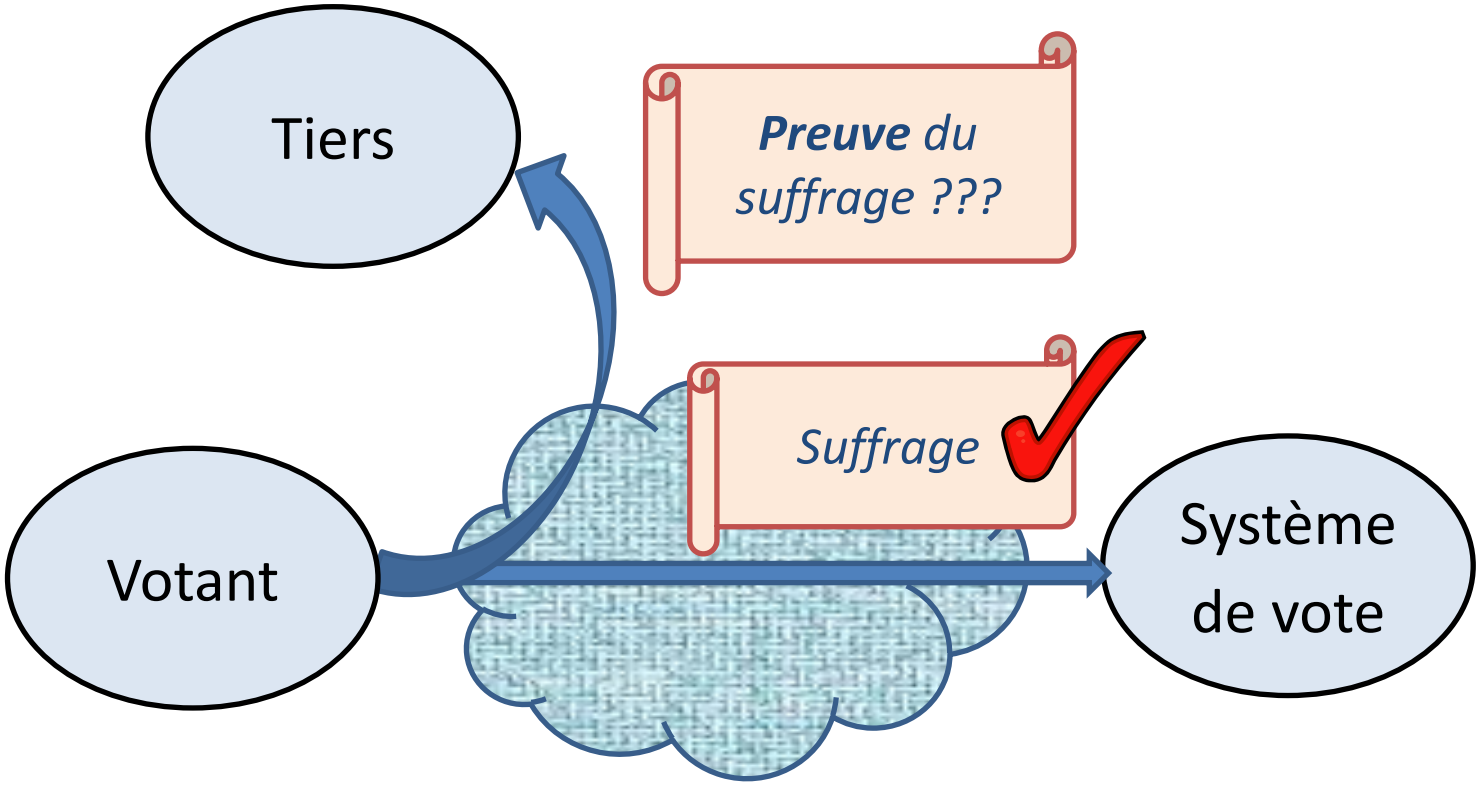


Propriétés

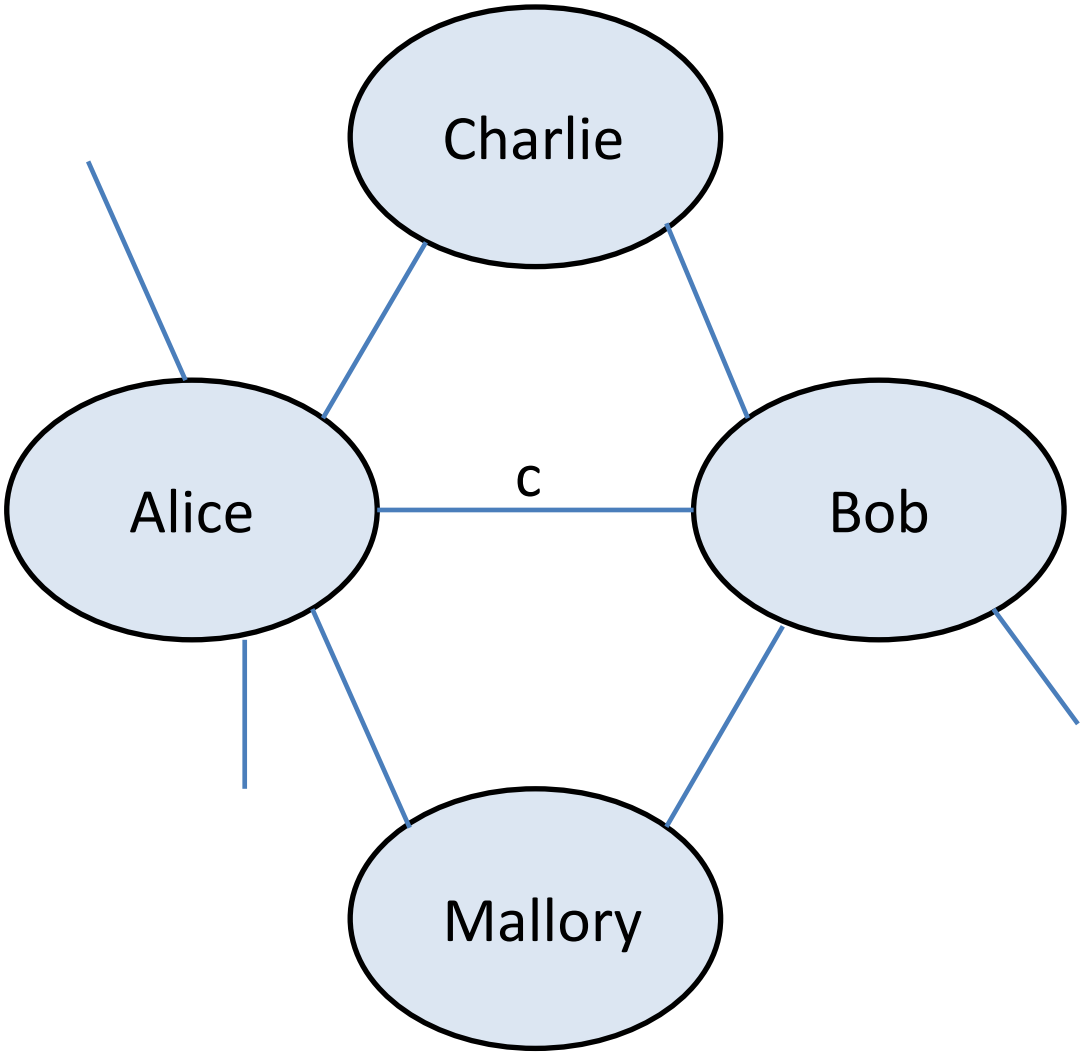
- *Intégrité* (ou *authenticité*).
- *Secret* (ou *confidentialité*).
- *Disponibilité*.




Votant
Suffrage
Système
de vote


Tiers
Preuve du suffrage ???
Suffrage
Votant
Système de vote

Alice et Bob au pays du pi calcul


Charlie
Alice
c
Bob
Mallory

Alice et Bob définis en pi calcul

Alice = $\overline{c}\langle M\rangle$

Bob = $c(x).Q$

Système = $(\nu\ c)\ (\text{Alice} \mid \text{Bob})$

$= (\nu\ c)\ (\overline{c}\langle M\rangle \mid c(x).Q)$

Alice et Bob définis en pi calcul

Alice = $\overline{c}\langle M\rangle$ *« envoyer M sur le canal c »*

Bob = c(x).Q

Système = (ν c) (Alice | Bob)

= (ν c) ($\overline{c}\langle M\rangle$ | c(x).Q)

Alice et Bob définis en pi calcul

Alice = $\overline{c}\langle M \rangle$ *« envoyer M sur le canal c »*

Bob = c(x).Q *« recevoir x sur le canal c, puis lancer Q »*

Système = $(\nu\ c)$ (Alice | Bob)

= $(\nu\ c)$ ($\overline{c}\langle M \rangle$ | c(x).Q)

Alice et Bob définis en pi calcul

Alice = $\overline{c}\langle M \rangle$ *« envoyer M sur le canal c »*

Bob = c(x).Q *« recevoir x sur le canal c, puis lancer Q »*

Système = $(\nu\ c)\ (\text{Alice} \mid \text{Bob})$

$= (\nu\ c)\ (\overline{c}\langle M \rangle \mid c(x).Q)$

« avec un canal c frais, lancer Alice et Bob en parallèle »

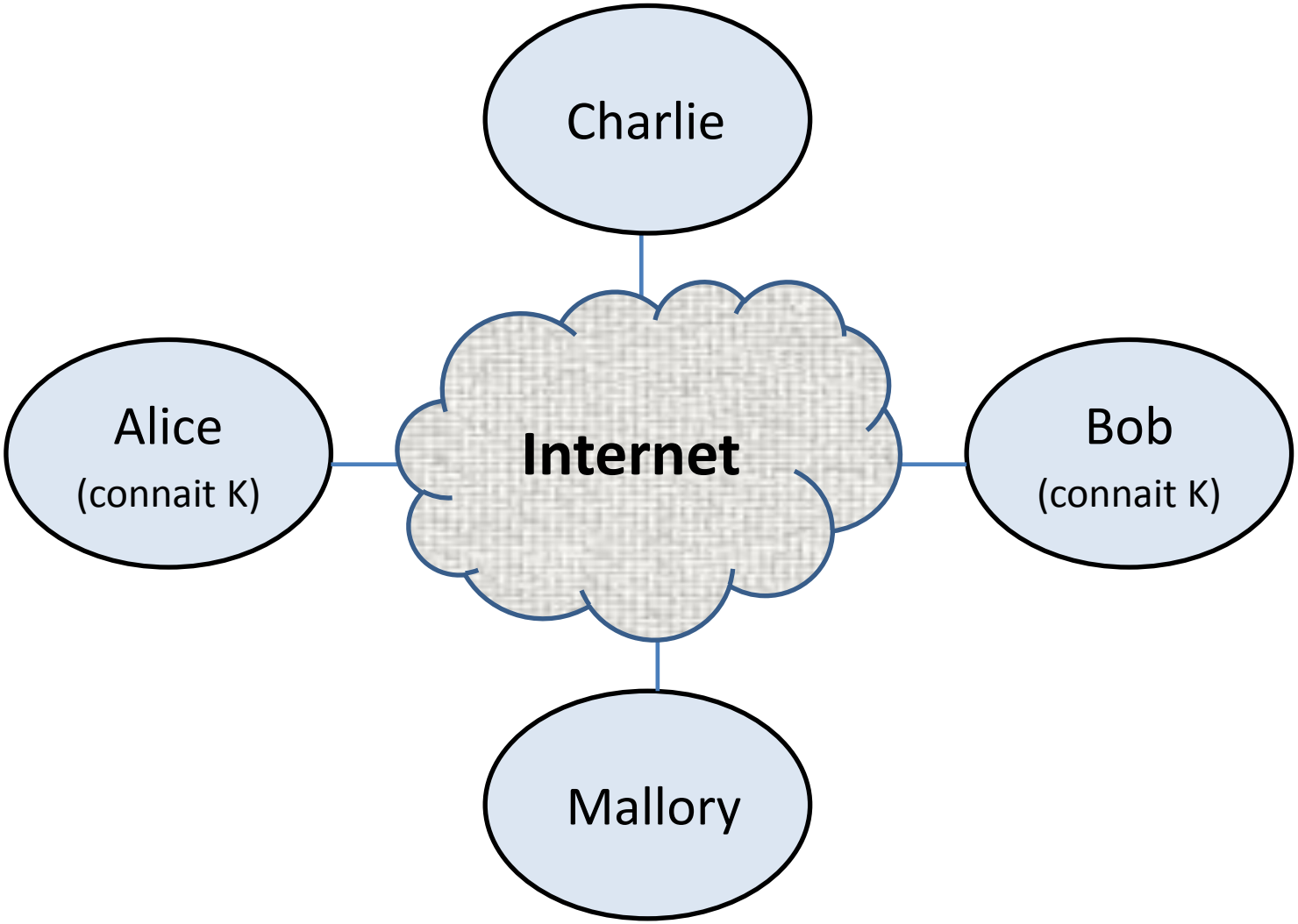
Communiquer en pi calcul

La communication est représentée par la réécriture:

$$(\nu\ c)\ (\overline{c}\langle M\rangle \mid c(x).Q) \rightarrow (\nu\ c)\ (Q \text{ avec } x = M)$$

La flèche → dénote une étape de calcul.
Puisque Alice = $\overline{c}\langle M\rangle$ et Bob = c(x).Q,
ceci équivaut à:

$$(\nu\ c)\ (\text{Alice} \mid \text{Bob}) \rightarrow (\nu\ c)\ (Q \text{ avec } x = M)$$


Charlie
Alice
(connait K)
Internet
Bob
(connait K)
Mallory

Alice et Bob redéfinis (avec chiffrement)

Alice = $\overline{\text{Internet}}\,\langle \text{chiffrer}(K,M) \rangle$

« envoyer M chiffré sous K, sur Internet »

Bob = Internet(y). soit x = déchiffrer(K,y). Q

« recevoir y sur Internet, le déchiffer avec K, en tirer x, puis lancer Q »

Système = (ν K) (Alice | Bob)

« avec une clef K fraîche, lancer Alice et Bob en parallèle »

Fonctionnement du chiffrement

chiffrer et déchiffrer sont des fonctions reliées par l'équation:

déchiffrer(K,chiffrer(K,M)) = M

qui implique que Bob retrouve bien M quand il déchiffre le message d'Alice.

Perte de la disponibilité

La disponibilité est perdue, puisque nous pouvons définir un processus récursif:

Gobeur = Internet(y). Gobeur

« recevoir y sur Internet,
puis recommencer »

qui est capable de recevoir tout message sur Internet et de l'absorber.

Sécurité du chiffrement

(pour l'intégrité et le secret)

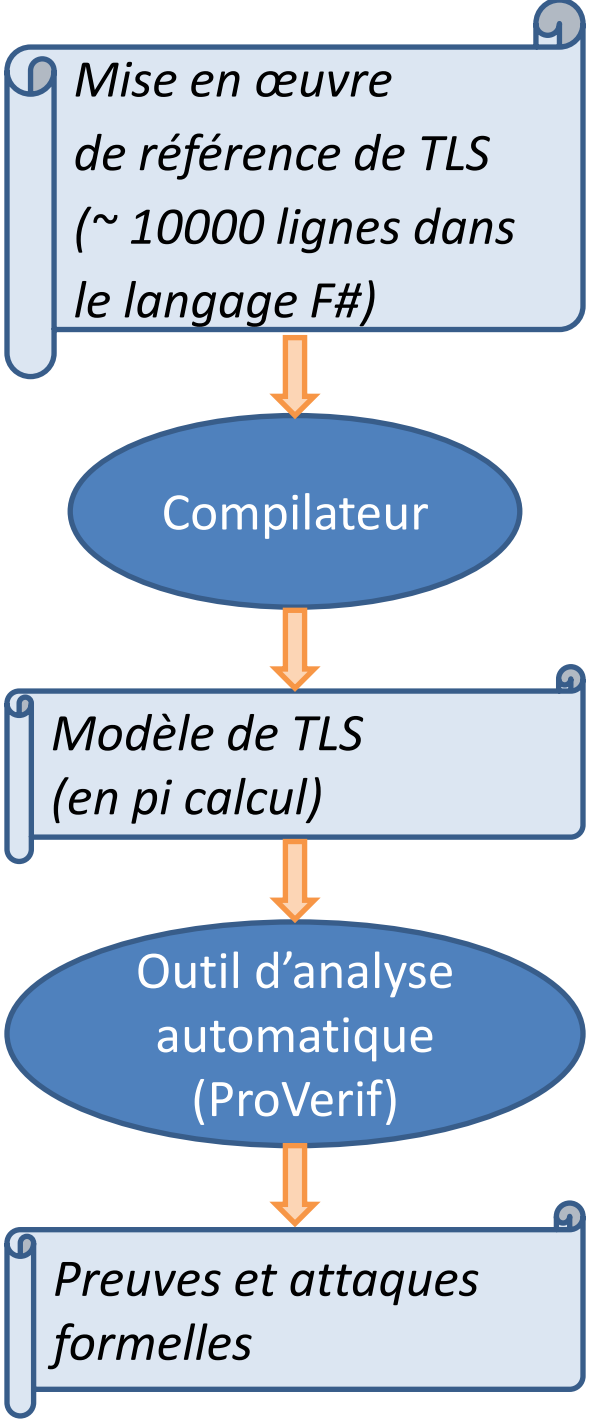
chiffrer et déchiffrer sont des fonctions reliées par l'équation:

déchiffrer(K,chiffrer(K,M)) = M

Il faut aussi que le chiffrement soit « sûr » (c'est-à-dire, qu'il protège bien M).

Une étude de cas: analyse symbolique du protocole TLS

[Bhargavan et al., 2008]



Difficulté du savoir

Study: Google-China attack driven by amateurs

By **Kevin Voigt**, CNN
March 3, 2010 2:35 a.m. EST

CNN

Google Hack Attack Was Ultra Sophisticated, New Details Show

By Kim Zetter ✉ January 14, 2010 | 8:01 pm | Categories: Breaches, Cybersecurity, Hacks and Cracks

WIRED

2 China Schools Said to Be Tied to Online Attacks

By JOHN MARKOFF and DAVID BARBOZA
Published: February 18, 2010

The New York Times nytimes.com

Page last updated at 22:48 GMT, Sunday, 24 January 2010

BBC Mobile

E-mail this to a friend Printable version

China rejects claims of cyber attacks on Google

Cyberattack on Google Said to Hit Password System

By JOHN MARKOFF
Published: April 19, 2010

The New York Times nytimes.com

From Times Online

January 18, 2010

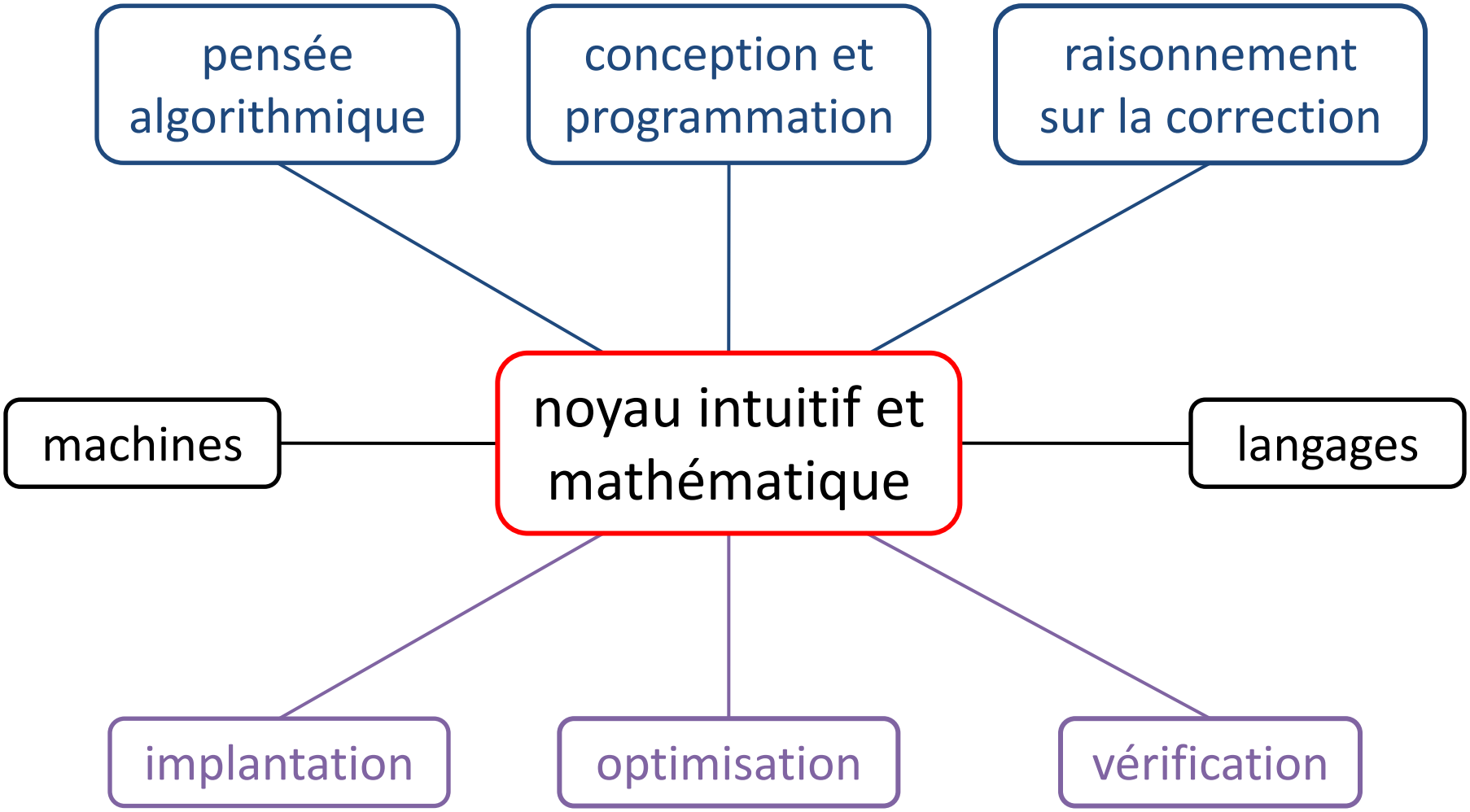
Google cyber-attack from China 'an inside job'

There are known knowns: there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns: the ones we don't know we don't know.

Rumsfeld

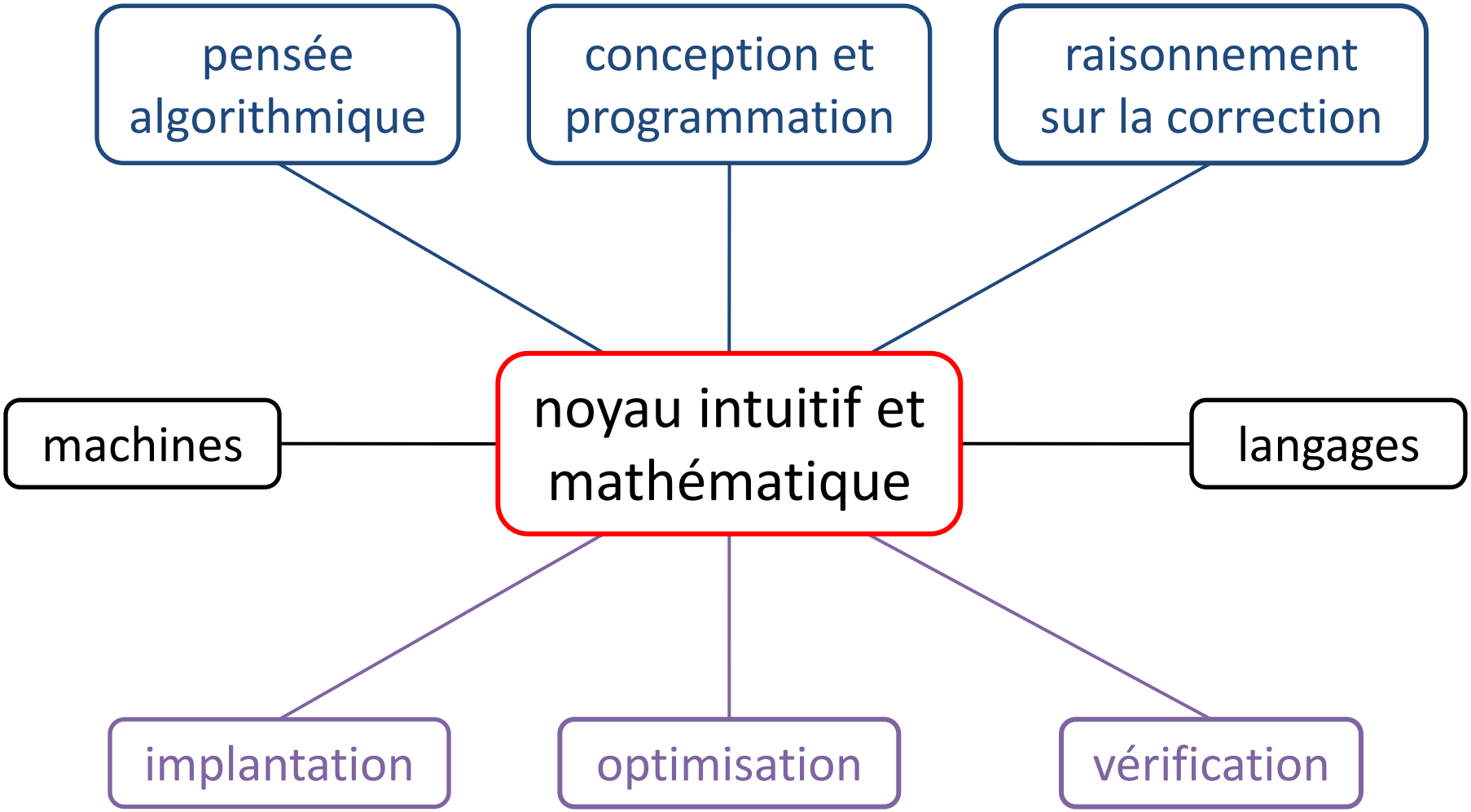
Anatomie d'un modèle de calcul

(d'après G. Berry)



Anatomie d'un modèle de calcul

(d'après G. Berry)



My message is that we must develop this logical theory; partly because otherwise the interactive systems which we build, or which just happen, will escape our understanding and the consequences may be serious, and partly because it is a new scientific challenge. Besides, it has all the charm of inventing the science of navigation while already on board ship.

Milner

Fin

Source gallica.bnf.fr / Bibliothèque nationale de France

Merci à Andrew Birrell, Andy Gordon, Brandon Enright, Bruno Blanchet, Butler Lampson, Cédric Fournet, David Pointcheval, Fabrice Fries, Fang Yu, Gérard Berry, Hubert Comon-Lundh, Jacques Stern, Jean Goubault-Larrecq, Jean-Jacques Lévy, Jean-Jacques Rosat, Jean-Philippe Martin, Marcelo Abadi, Marie Chéron, Mathieu Baudet, Miguel Helft, Mike Schroeder, Ross Anderson, Serge Abiteboul, Stefan Savage, Ted Wobber, Véronique Cortier et Yinglian Xie