Les protocoles cryptographiques: comment sécuriser nos communications ?

Stéphanie Delaune

Chargée de recherche CNRS au LSV,

INRIA projet Secsi & ENS Cachan

21 Mai 2008

ENS Cachan

- 17 départements d'enseignement: mathématiques, informatique, chimie, génie mécanique, sciences sociales, ...
- 12 laboratoires de recherche: Laboratoire Spécification & Vérification, ...

La recherche au LSV

$\longrightarrow$ accroître notre confiance dans les logiciels critiques

La recherche au LSV

$\longrightarrow$ accroître notre confiance dans les logiciels critiques

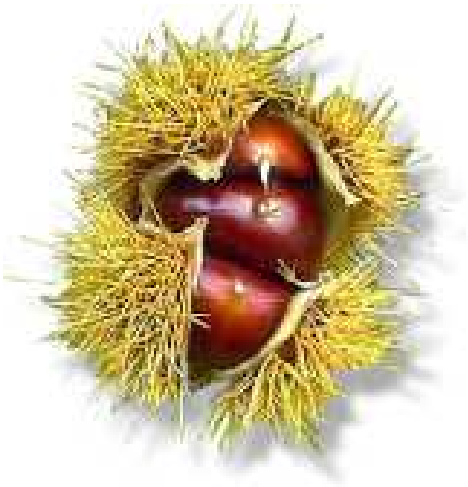
- logiciel: texte relativement long écrit dans un langage spécifique et qui sera exécuté par un ordinateur
- critique: une défaillance peut avoir des conséquences désastreuses en termes humains ou économiques

La recherche au LSV

Ennemi public numéro 1: le bug ...

La recherche au LSV

Ennemi public numéro 1: le bug ...



... aussi connu sous le nom de bogue !

Dans la vie quotidienne !

Dans la vie quotidienne !

Ariane V - 4 juin 1996

Un crash après 40 secondes de vol dû

...

Ariane V - 4 juin 1996

Un crash après 40 secondes de vol dû

...

à un bug logiciel !

1. 189 vols réussis pour Ariane IV,
2. réutilisation du logiciel de lancement d'Ariane IV,
3. ajout du nécessaire pour la nouvelle fusée.

$\longrightarrow$ Le logiciel d'Ariane IV contenait un bug !

Sonde Mars Climate Orbiter - 26 septembre 1999

Perte de la sonde due ...

Sonde Mars Climate Orbiter - 26 septembre 1999

Perte de la sonde due ... à un problème d'unité de mesure !

Carte bancaire

La carte bleue est protégée par un grand nombre public dont on ne connait pas la factorisation.

Carte bancaire

La carte bleue est protégée par un grand nombre public dont on ne connait pas la factorisation.

Nombre de 96 chiffres

213598703592091008239502270499962879705109534182641740644252
416500858395774644508840500943086599 9

Carte bancaire

La carte bleue est protégée par un grand nombre public dont on ne connait pas la factorisation.

Nombre de 96 chiffres

213598703592091008239502270499962879705109534182641740644252
416500858395774644508840500943086599 9

Affaire Serge Humpich (1997)

il factorise ce nombre de 96 chiffres et conçoit de fausses cartes bleues (les « YesCard »).

Carte bancaire

La carte bleue est protégée par un grand nombre public dont on ne connait pas la factorisation.

Nombre de 96 chiffres

213598703592091008239502270499962879705109534182641740644252
416500858395774644508840500943086599 9

Affaire Serge Humpich (1997)

il factorise ce nombre de 96 chiffres et conçoit de fausses cartes bleues (les « YesCard »).

$\longrightarrow$ Depuis, le nombre utilisé pour sécuriser les cartes bancaires comportent 232 chiffres.

Difficultés et enjeux

$\longrightarrow$ une petite modification (quelques caractères) peut le transformer complètement.

Un besoin crucial de vérification

- pour des raisons économiques
  $\longrightarrow$ Ariane 5, carte bancaire, ...
- mais parfois il y a aussi des vies humaines en jeu
  $\longrightarrow$ la machine Therac-25 dans les années 80
  $\longrightarrow$ logiciels embarqués dans les voitures, les avions, ...

Comment fait-on ?

Tests

- à la main ou génération automatique;
- vérification d'un nombre fini de cas.

Comment fait-on ?

Tests

- à la main ou génération automatique;
- vérification d'un nombre fini de cas.

$\infty \infty \infty$ Accéder à l'infini: un rêve impossible ? $\infty \infty \infty$

Comment fait-on ?

Tests

- à la main ou génération automatique;
- vérification d'un nombre fini de cas.

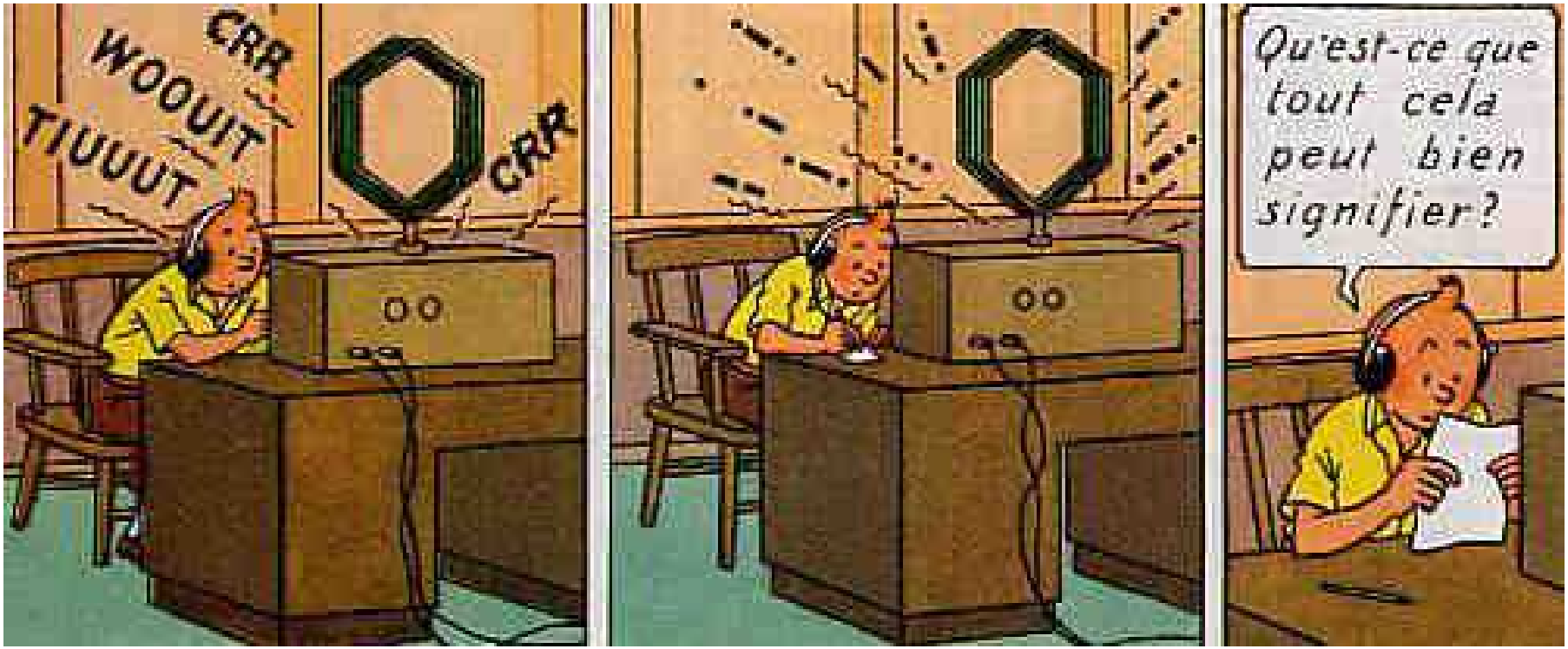
$\infty \infty \infty$ Accéder à l'infini: un rêve impossible ? $\infty \infty \infty$

Vérification (preuves formelles)

$\longrightarrow$ preuves mathématiques

- à la main ou à l'aide d'ordinateur;
- vérification de tous les cas possibles;
- plus difficile.

Les protocoles cryptographiques:
comment sécuriser nos communications ?



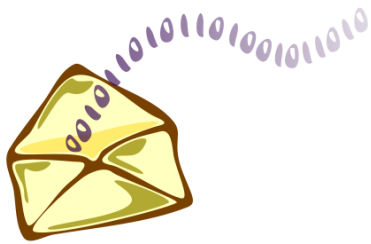
Les protocoles cryptographiques

- petits programmes destinés à sécuriser les communications
- omniprésents: paiement sur internet, e-administration (impôts), distributeurs de billets, téléphonie mobile. . .

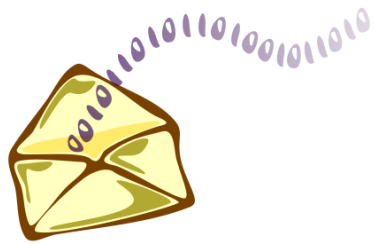
Internet

Le réseau de communication est non fiable !

Une ville imaginaire ....



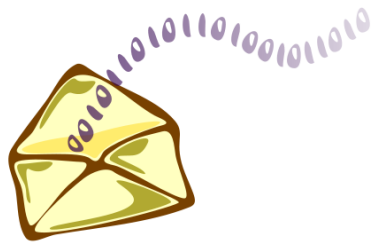
Une ville imaginaire ....



... mais le postier est malhonnête, il

- peut intercepter les messages,
- peut changer le nom de l'expéditeur du courrier,
- peut distribuer des faux messages,
- ...

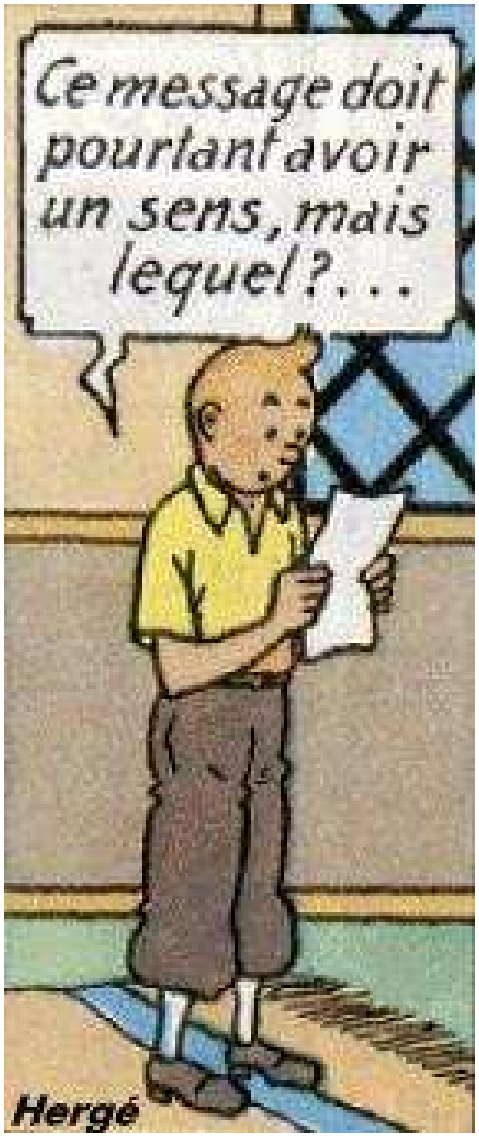
Une ville imaginaire ....



... mais le postier est malhonnête, il

- peut intercepter les messages,
- peut changer le nom de l'expéditeur du courrier,
- peut distribuer des faux messages,
- ...

Il faut protéger les messages !

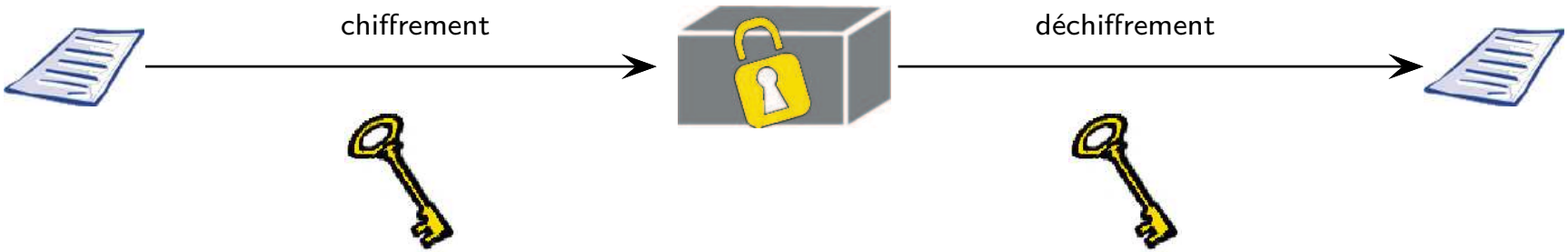


Le chiffrement

« ROBPS LDGHV GHPDW
KHPDW LTXHV »

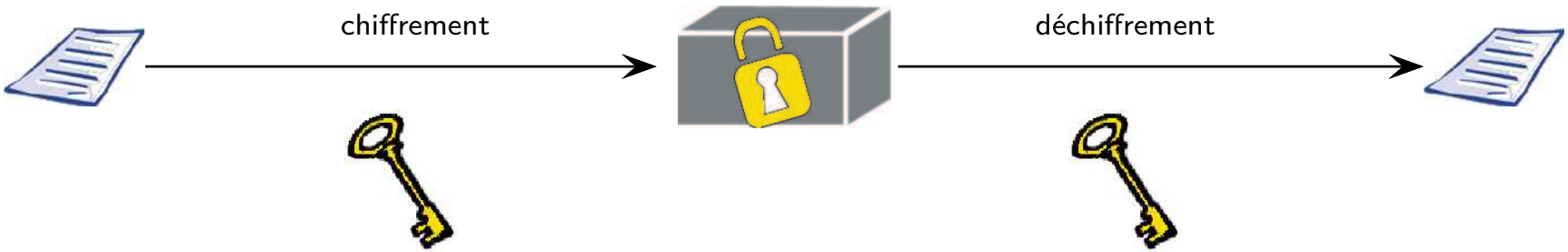
Qu'est-ce que le chiffrement ?

Chiffrement Symétrique



Qu'est-ce que le chiffrement ?

Chiffrement Symétrique



- plus ancienne forme de chiffrement,
- traces de son utilisation par les Égyptiens vers 2000 avant J.-C.

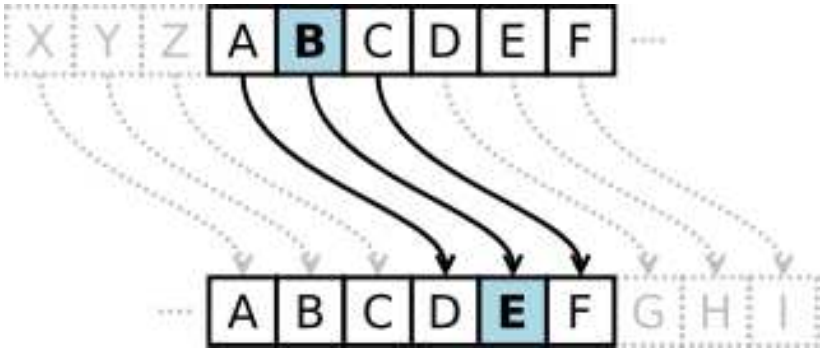
Chiffrement de César

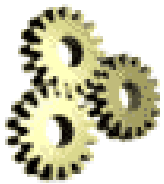
Cette méthode consiste à décaler les lettres de l'alphabet d'un nombre fixé de crans

Chiffrement de César

Cette méthode consiste à décaler les lettres de l'alphabet d'un nombre fixé de crans

Exemple: Un décalage de 3.



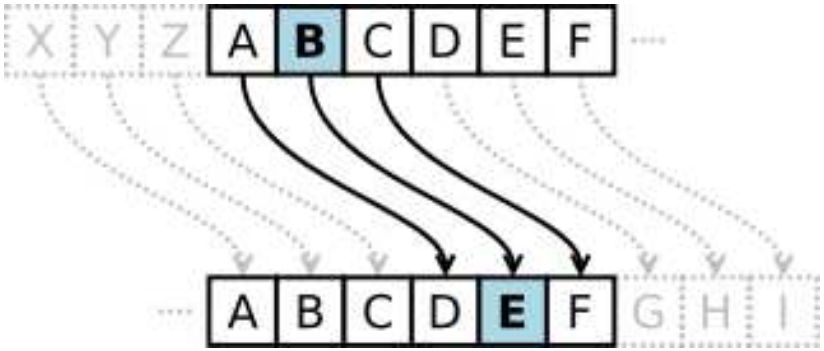


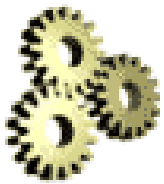
OLYMPIADES DE MATHEMATIQUES

Chiffrement de César

Cette méthode consiste à décaler les lettres de l'alphabet d'un nombre fixé de crans

Exemple: Un décalage de 3.





OLYMPIADES DE MATHEMATIQUES

ROBPS LDGHV GHPDW KHPDW LTXHV

Seconde Guerre mondiale (1939-1945)

Enigma

- machine électro-mécanique portable d'origine allemande,
- nombreuses permutations.

Un peu d'histoire ...

- 1945: La plupart des messages codés allemands étaient décryptés en un jour ou deux.
- Alan Turing a beaucoup contribué à « casser » cette méthode de chiffrement.

Seconde Guerre mondiale (1939-1945)

Enigma

- machine électro-mécanique portable d'origine allemande,
- nombreuses permutations.

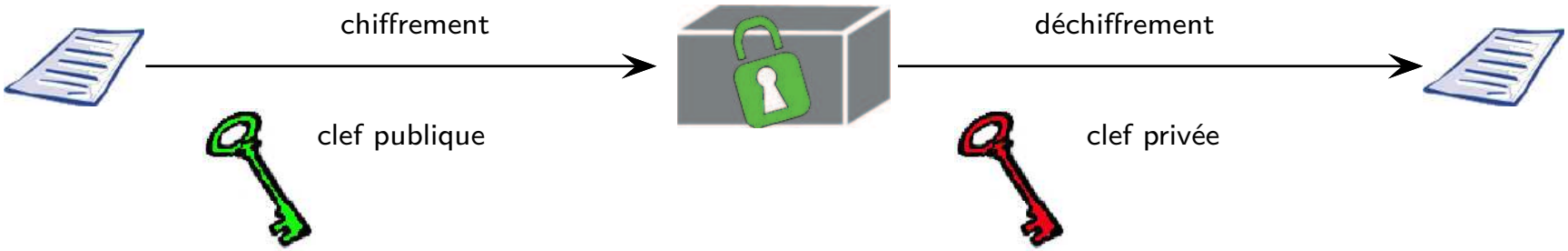
Un peu d'histoire ...

- 1945: La plupart des messages codés allemands étaient décryptés en un jour ou deux.
- Alan Turing a beaucoup contribué à « casser » cette méthode de chiffrement.

$\longrightarrow$ aujourd'hui, le DES (développé par IBM) utilise les mêmes ingrédients

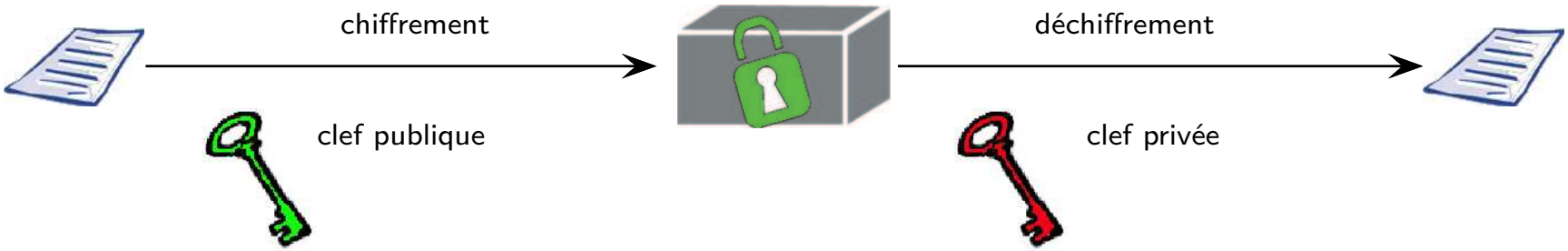
Chiffrement asymétrique (ou à clefs publiques)

Chiffrement asymétrique



Chiffrement asymétrique (ou à clefs publiques)

Chiffrement asymétrique

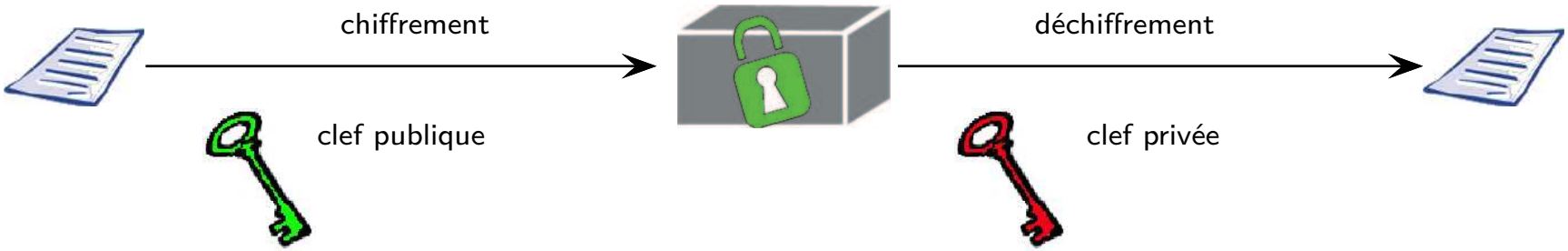


1977: chiffrement RSA (encore utilisé à l'heure actuelle)

- cette méthode de chiffrement repose sur un problème mathématique bien connu: le problème de la factorisation.

Chiffrement asymétrique (ou à clefs publiques)

Chiffrement asymétrique



1977: chiffrement RSA (encore utilisé à l'heure actuelle)

- cette méthode de chiffrement repose sur un problème mathématique bien connu: le problème de la factorisation.

Tant que nous ne sommes pas capables de résoudre ce problème d'une façon efficace, la méthode de chiffrement RSA sera considérée sûre.

Casser le chiffrement RSA

Les challenges RSA

- défis lancés par le laboratoire RSA Security
- récompenses importantes offertes

Casser le chiffrement RSA

Les challenges RSA

- défis lancés par le laboratoire RSA Security
- récompenses importantes offertes

RSA-576	174 chiffres	réussi	2003
RSA-640	193 chiffres	réussi	2005
RSA-704	212 chiffres	non résolu – 30 000 dollars	
...	..	...	
RSA-2048	617 chiffres	non résolu – 200 000 dollars	

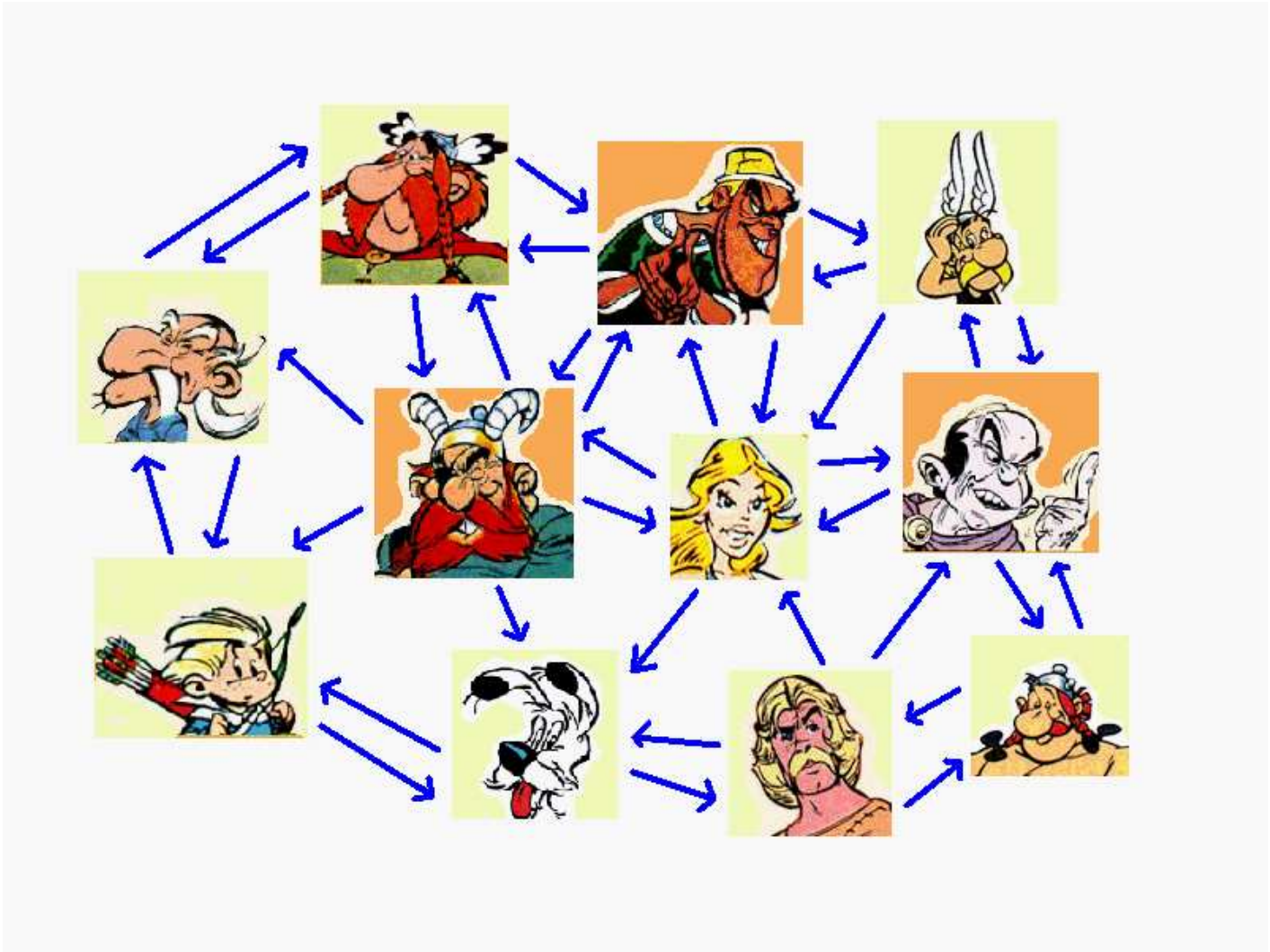
Casser le chiffrement RSA

Les challenges RSA

- défis lancés par le laboratoire RSA Security
- récompenses importantes offertes

RSA-576	174 chiffres	réussi	2003
RSA-640	193 chiffres	réussi	2005
RSA-704	212 chiffres	non résolu – 30 000 dollars	
...	..	...	
RSA-2048	617 chiffres	non résolu – 200 000 dollars	

$\longrightarrow$ Ces challenges ont été retirés en 2007 !



Chiffrer ne suffit pas toujours !

Attaque par rejeu de messages

virer 100 euros sur
le compte du marchand

Attaque par rejeu de messages

virer 100 euros sur
le compte du marchand

virer 100 euros sur

le compte du marchand

Attaque par rejeu de messages

virer 100 euros sur
le compte du marchand

virer 100 euros sur
le compte du marchand

virer 100 euros sur
le compte du marchand

⋮

virer 100 euros sur
le compte du marchand

Attaque par rejeu de messages

virer 100 euros sur
le compte du marchand

virer 100 euros sur
le compte du marchand

virer 100 euros sur
le compte du marchand

⋮

virer 100 euros sur
le compte du marchand

Exemple: attaque sur les décodeurs (bloquer l'ordre de désabonnement)

Retour sur le protocole de carte bancaire

- Le client Cl insère sa carte C dans le terminal T.
- Le marchand saisit le montant M de la transaction.

- Le terminal vérifie qu'il s'agit d'une « vraie carte ».
- Le client entre son code.
  Si $M \geq$ €100, alors dans 20% des cas,
  - Le terminal contacte la banque B.
  - La banque donne (ou pas) son autorisation.

En détails

Le terminal T lit la carte C:

1. $C \rightarrow T : Data, \{Data\}_{\mathsf{priv}(B)}$

En détails

Le terminal T lit la carte C:

1. $C \rightarrow T$: $Data, \{Data\}_{\mathsf{priv}(B)}$

Le terminal T demande le code:

2. $T \rightarrow CI$: $code?$
3. $CI \rightarrow C$: 1234
4. $C \rightarrow T$: code bon

En détails

Le terminal T lit la carte C:

1. $C \rightarrow T$: $Data, \{Data\}_{priv(B)}$

Le terminal T demande le code:

2. $T \rightarrow CI$: *code?*
3. $CI \rightarrow C$: 1234
4. $C \rightarrow T$: code bon

Le terminal T demande l'autorisation à la banque B:

5. $T \rightarrow B$: *autorisation?*
6. $B \rightarrow T$: 45289
7. $T \rightarrow C$: 45289
8. $C \rightarrow T$: $\{45289\}_{K_{CB}}$
9. $T \rightarrow B$: $\{45289\}_{K_{CB}}$
10. $B \rightarrow T$: *ok*

Attaques sur la carte bleue

Initialement la sécurité été assurée par :

- cartes difficilement réplicables,
- secret des clefs et du protocole.

Attaques sur la carte bleue

Initialement la sécurité été assurée par :

- cartes difficilement réplicables,
- secret des clefs et du protocole.

Mais il y a des failles !

- le chiffrement n'est pas sûr;
- on peut faire des fausses cartes.

→ "YesCard" fabriquées par Serge Humpich (1997).

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Notre but:

1. faire des preuves mathématiques rigoureuses,
2. d'une façon automatique.

« Construire une machine à détecter les bugs »

Comment vérifier ces protocoles ?

Les mathématiques et l'informatique à la rescousse !

Notre but:

1. faire des preuves mathématiques rigoureuses,
2. d'une façon automatique.

« Construire une machine à détecter les bugs »

1936: une telle machine n'existe pas (Alan Turing)

... même dans le cas particulier des protocoles cryptographiques.

Mais alors, que faisons nous ?

Le problème n'a pas de solution ....

Mais alors, que faisons nous ?

Le problème n'a pas de solution ....

mais seulement dans le cas général

Mais alors, que faisons nous ?

Le problème n'a pas de solution ....

mais seulement dans le cas général

Différentes pistes:

- résoudre le problème dans de nombreux cas intéressants,

Mais alors, que faisons nous ?

Le problème n'a pas de solution ....

mais seulement dans le cas général

Différentes pistes:

- résoudre le problème dans de nombreux cas intéressants,
- proposer des procédures approchées,

  Exemple: si le vérificateur répond « oui » alors le logiciel est sûr, sinon on ne peut rien dire

Mais alors, que faisons nous ?

Le problème n'a pas de solution ....

mais seulement dans le cas général

Différentes pistes:

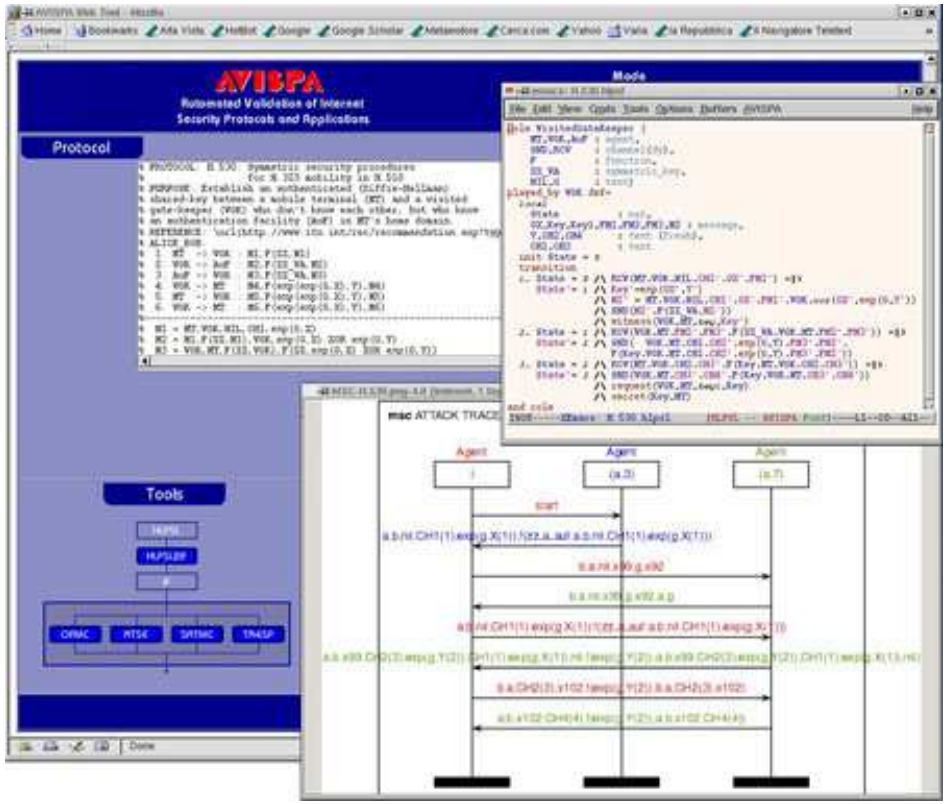
- résoudre le problème dans de nombreux cas intéressants,
- proposer des procédures approchées,

  Exemple: si le vérificateur répond « oui » alors le logiciel est sûr, sinon on ne peut rien dire

- ...

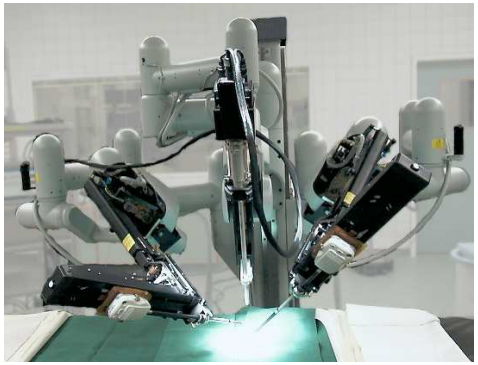
Outil de vérification AVISPA

Outil disponible en ligne: `http://www.avispa-project.org/`



$\longrightarrow$ Projet Européen (France, Italie, Allemagne, Suisse)

Il reste beaucoup à faire

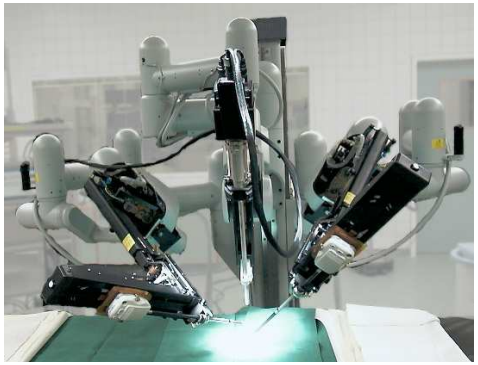


Les logiciels sont en perpétuelle évolution ...

- en vue de leur amélioration,
- pour développer de nouvelles applications
  $\longrightarrow$ vote électronique, robot en chirurgie, ...

... et sont de plus en plus complexes.

Il reste beaucoup à faire



Les logiciels sont en perpétuelle évolution ...

- en vue de leur amélioration,
- pour développer de nouvelles applications
  $\longrightarrow$ vote électronique, robot en chirurgie, ...

... et sont de plus en plus complexes.

L'informatique est une discipline très vaste et en plein essor.

- informatique de la vérification,
- bioinformatique,
- exploration de données, ...