ELHQY HQXHD ODWHO LHUGH
FUBSW RJUDS KLH

Déchiffrez tous les codes secrets !

Concours ALKINDI

2021 – 2022

Ouvert aux 4e, 3e et 2de

Inscription gratuite

WWW.CONCOURS-ALKINDI.FR

Concours de cryptanalyse organisé par les associations Animath et France-ioi. Participation gratuite, en ligne.
Inscription à effectuer sur notre site par un·e enseignant·e jusqu'à la fin du premier tour, qui aura lieu du 6 au 17 décembre 2021.

Conception graphique : Sedeto.fr – Illustration : @Aadorah

MINISTÈRE DE L'ÉDUCATION NATIONALE, DE LA JEUNESSE ET DES SPORTS

France IOI

Animath
Association pour l'animation mathématique

DGSE

Inria

La vérification formelle appliquée aux protocoles cryptographiques

Stéphanie Delaune

Univ Rennes, CNRS, IRISA

Janvier 2022

Les protocoles cryptographiques sont partout !

$\longrightarrow$ sécuriser nos communications : authentification sur les services de banque en ligne, confidentialité des données échangées, protection de nos données personnelles, ...

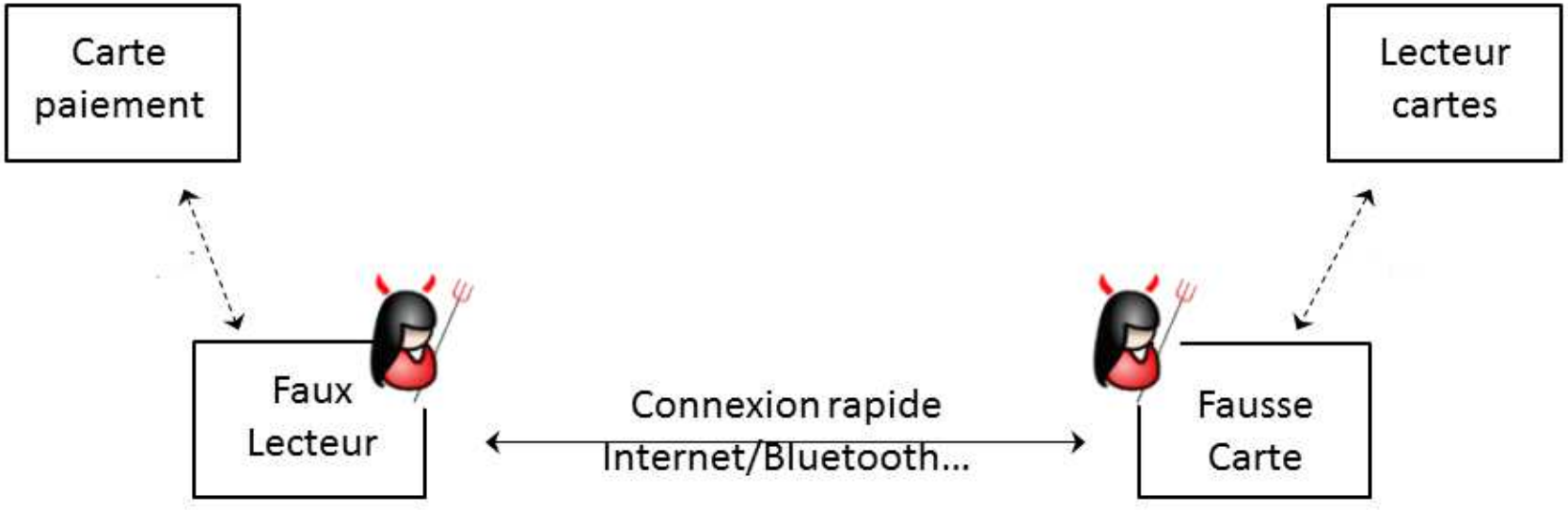
Le paiement sans contact ...

Plus de 30 millions de cartes de paiement sans contact sont en circulation en France.

Le paiement sans contact ...

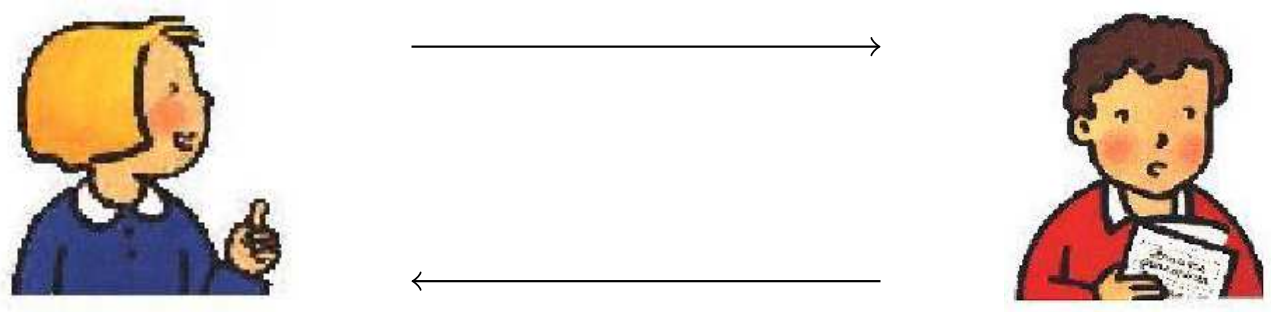
Plus de 30 millions de cartes de paiement sans contact sont en circulation en France.

... est vulnérable à l'attaque par relais :



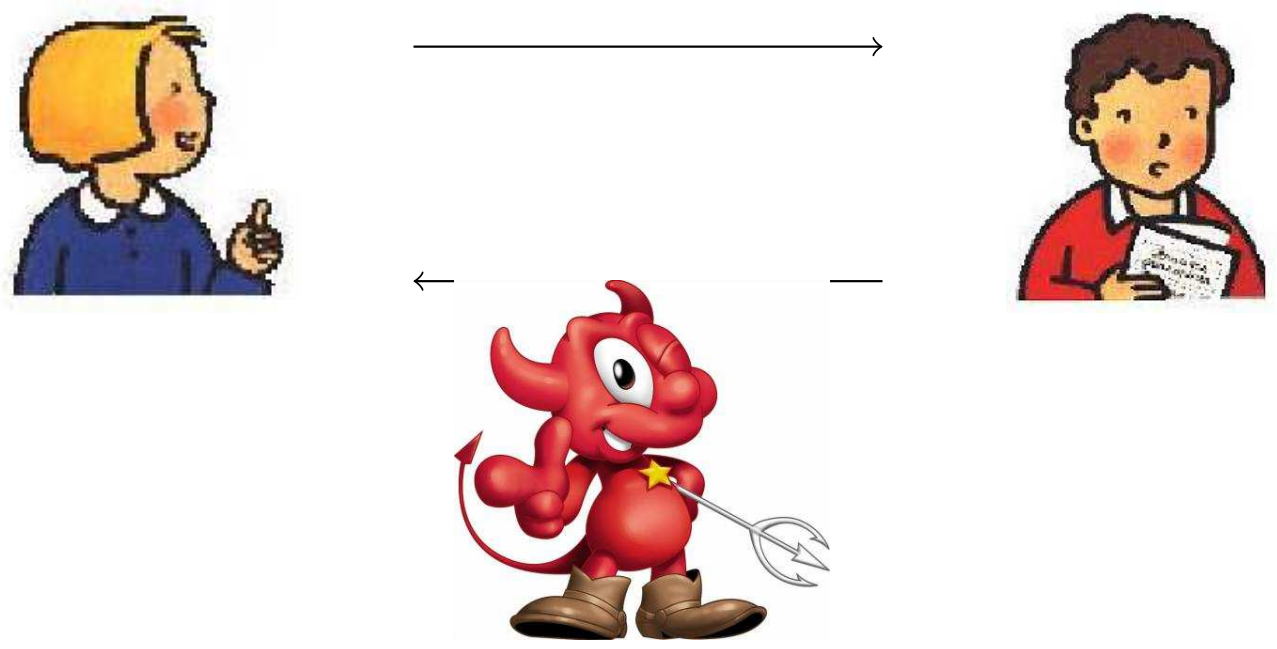
Problème : aucun dispositif ne permet d'assurer la proximité physique de la carte qui réalise la transaction.

Un protocole cryptographique : qu'est-ce que c'est ?



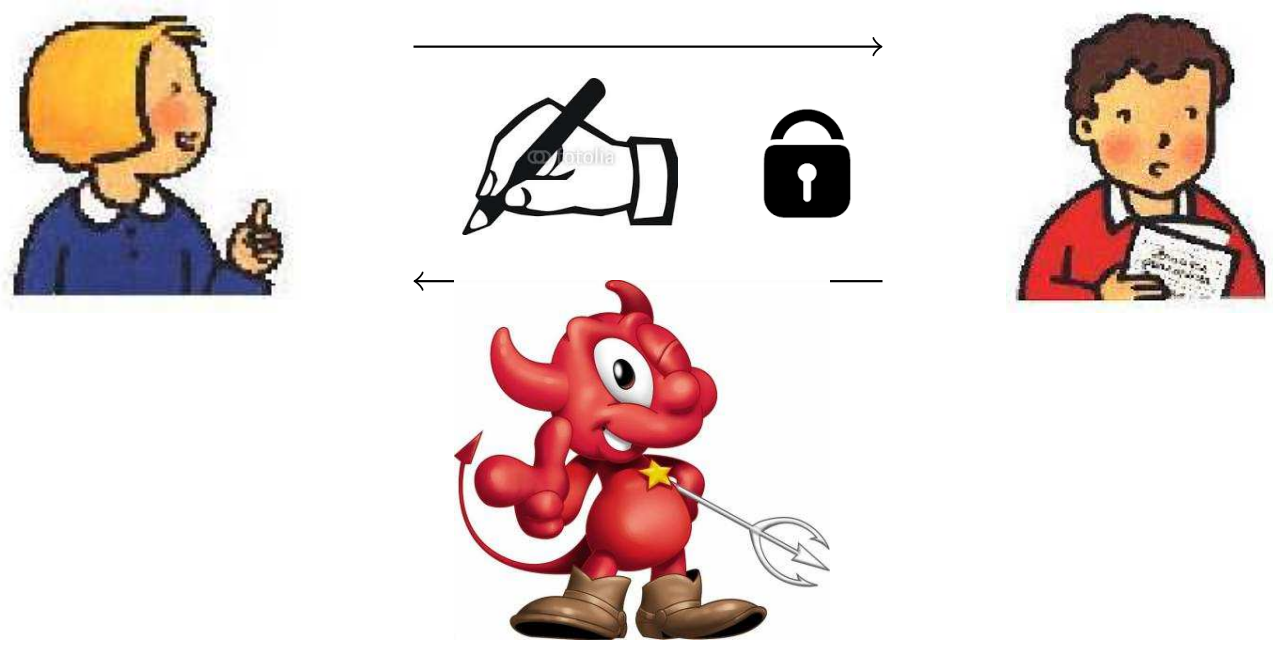
- Protocole : petit programme explicitant les messages échangés

Un protocole cryptographique : qu'est-ce que c'est ?



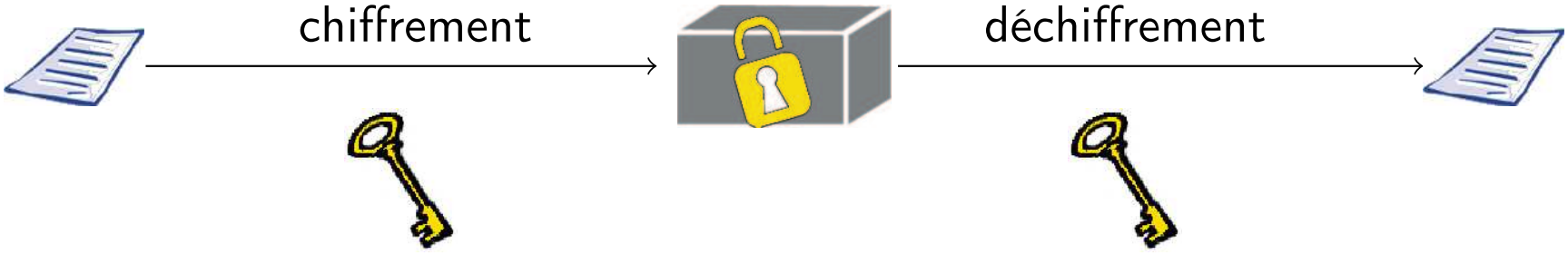
- Protocole : petit programme explicitant les messages échangés

Un protocole cryptographique : qu'est-ce que c'est ?

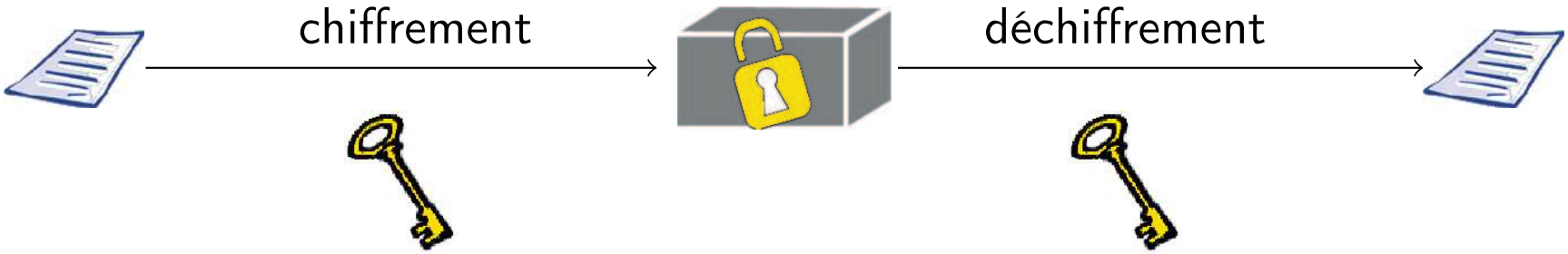


- Protocole : petit programme explicitant les messages échangés
- Cryptographique : utilisant des primitives cryptographiques (e.g. chiffrement symétrique, asymétrique, signature, . . .)

Chiffrement symétrique

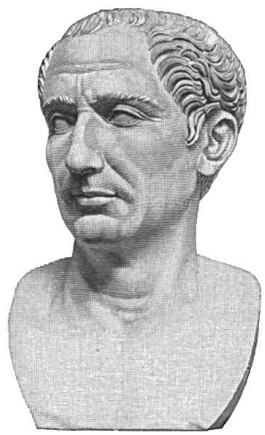


Chiffrement symétrique



scytale (400 av. JC)

César (50 av. JC)

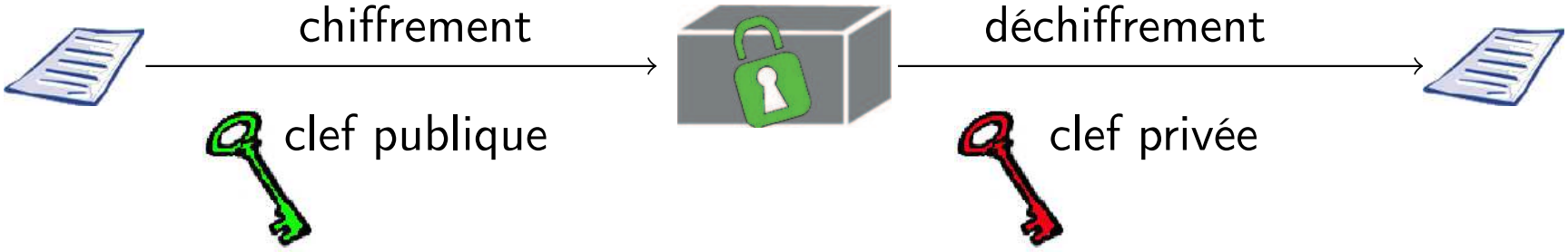


Enigma (1940)

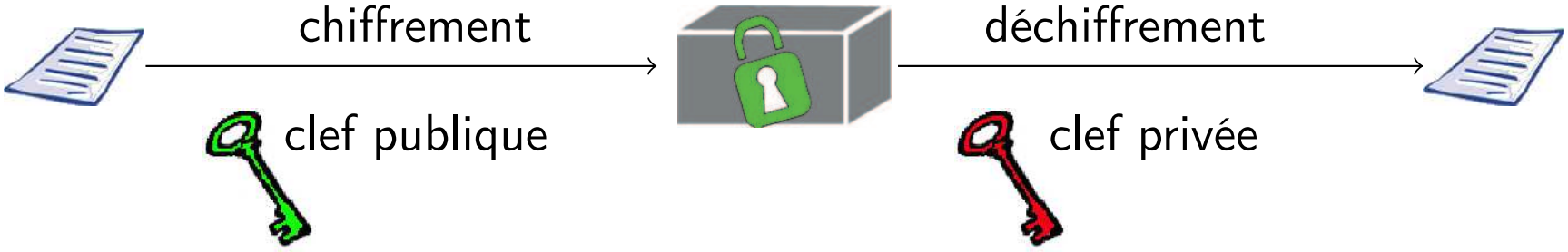
Quelques algorithmes plus récents :

- Data Encryption Standard (1977) ;
- Advanced Encryption Standard (2000).

Chiffrement asymétrique

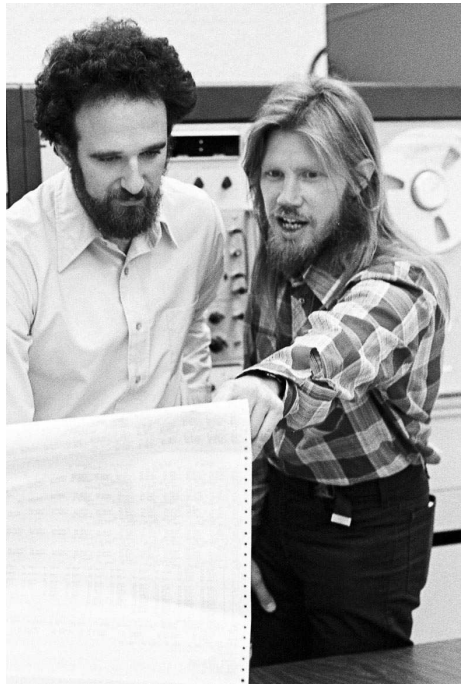


Chiffrement asymétrique



Quelques exemples :

- 1976 : 1er système
  W. Diffie et M. Hellman
  $\longrightarrow$ Prix Turing 2016
- 1977 : système RSA
  R. Rivest, A. Shamir, et L. Adleman



$\longrightarrow$ Ces systèmes sont toujours utilisés de nos jours.

Les protocoles utilisés de nos jours ...

... comportent de nombreuses failles qualifiées de logiques.

Connexion HTTPS — Barghavan et al. 2015

Une attaque du type “homme du milieu“ permet de faire revivre un vieux mode de chiffrement.

$\longrightarrow$ environ 10% des sites sont vulnérables

`https://freakattack.com`

Passeport électronique — Chothia et al. 2010

Des messages d'erreurs trop précis permettent de tracer le porteur d'un passeport français.

Carte bancaire

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

Nombre de 96 chiffres

213598703592091008239502270499962879705109534182641740644252416500858395774644508840500943086599

Carte bancaire

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

Nombre de 96 chiffres

21359870359209100823950227049996287970510953
41826417406442524165008583957746445088405009430865999

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
21359870359209100823950227049996287970510953
41826417406442524165008583957746445088405009430865999

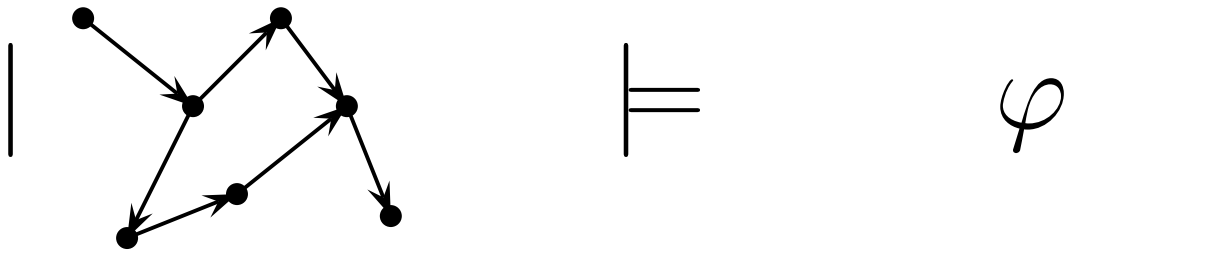
Affaire Serge Humpich (1997)
il factorise ce nombre de 96 chiffres et conçoit de fausses cartes bleues (les « YesCard »).

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

La vérification formelle appliquée aux protocoles cryptographiques

Est-ce que le protocole *satisfait* la propriété de sécurité ?

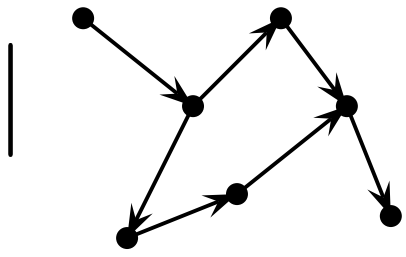
Modélisation



La vérification formelle appliquée aux protocoles cryptographiques

Est-ce que le protocole *satisfait* la propriété de sécurité ?

Modélisation



$\models$ φ

Deux tâches principales

1. Modélisation : protocoles, propriétés de sécurité, sans oublier notre adversaire !
2. Mise au point d'algorithmes de vérification.

Comment vérifier ces protocoles ?

Notre but :

- faire des preuves mathématiques rigoureuses ;
- d'une façon automatique.

Construire une machine à détecter les bugs !

Comment vérifier ces protocoles ?

Notre but :

- faire des preuves mathématiques rigoureuses ;
- d'une façon automatique.

Construire une machine à détecter les bugs !

A. Turing (1936)

Une telle machine n'existe pas ...

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

Mais alors que faisons nous ?

Des procédures approchées pour la preuve de protocoles :

- outil ProVerif basé sur la résolution de clauses de Horn
- outil Tamarin (avec un mode interactif)
- outil Squirrel pour faire de la preuve interactive et obtenir des garanties fortes dans le modèle dit calculatoire

Mais alors que faisons nous ?

Des procédures approchées pour la preuve de protocoles :

- outil ProVerif basé sur la résolution de clauses de Horn
- outil Tamarin (avec un mode interactif)
- outil Squirrel pour faire de la preuve interactive et obtenir des garanties fortes dans le modèle dit calculatoire

Des procédures dédiées à la recherche d'attaques :

- outil SATMC basé sur les solveurs SAT
- outils OFMC et APTE basés sur la résolution de systèmes de contraintes

$\longrightarrow$ Ces procédures sont complètes pour certaines classes de protocoles et de scénarios (nombre borné de sessions).

Conclusion

À retenir

Les protocoles cryptographiques sont :

- difficiles à concevoir et à analyser ;
- vulnérables aux attaques logiques.

Des primitives robustes, c'est bien . . .

. . . **mais ce n'est pas suffisant !**

À retenir

Les protocoles cryptographiques sont :

- difficiles à concevoir et à analyser ;
- vulnérables aux attaques logiques.

Il est important de s'assurer du bon fonctionnement de ces protocoles.

Ce que l'on sait faire :

- les propriétés de sécurité les plus classiques ;
- l'analyse de protocoles plutôt petits ;
- les primitives cryptographiques standard.

De nombreuses pistes à explorer

Au vu des applications qui voient le jour, **ce n'est pas suffisant !**

- nouveaux objectifs de sécurité
  $\longrightarrow$ anonymat, non traçabilité, proximité physique, ...
- propriétés algébriques
  $\longrightarrow$ chiffrement homomorphe, ou exclusif, ...
- passage à l'échelle
  $\longrightarrow$ une même application est généralement composée de plusieurs protocoles

Questions ?