Pourquoi chiffrer les informations ne suffit pas ?

Stéphanie Delaune

Chargée de recherche CNRS
IRISA, Équipe EMSEC

8 décembre 2016

Objectif : sécuriser nos communications

$\longrightarrow$ authentification sur les services de banque en ligne, confidentialité des données échangées, anonymat lors d'une procédure de vote en ligne, ...

Passeport électronique

Un passeport électronique est un passeport contenant une puce RFID.

$\longrightarrow$ ils sont délivrés en France depuis l'été 2006.

La puce RFID permet de stocker :

- les informations écrites sur le passeport,
- votre photo numérisée.

Passeport électronique

Un passeport électronique est un passeport contenant une puce RFID.

$\longrightarrow$ ils sont délivrés en France depuis l'été 2006.

La puce RFID permet de stocker :

- les informations écrites sur le passeport,
- votre photo numérisée.

Il est interrogeable à distance à l'insu de son propriétaire !

Passeport électronique

1ère Génération

Aucun mécanisme de sécurité pour protéger les informations personnelles

Passeport électronique — 1ère Génération

Aucun mécanisme de sécurité pour protéger les informations personnelles

$\longrightarrow$ possibilité de récupérer la signature du porteur en interrogeant le passeport à distance

Passeport électronique — 1ère Génération

Aucun mécanisme de sécurité pour protéger les informations personnelles

$\longrightarrow$ possibilité de récupérer la signature du porteur en interrogeant le passeport à distance

"Faille" découverte sur les passeports belges

Passeport émis entre 2004 et 2006 en Belgique

Que dire des autres applications ?

Le cas du passeport électronique n'est pas un cas isolé !

Grand format : des puces électroniques partout
JT de 20h du 4 décembre 2016 sur France 2

Que dire des autres applications ?

Le cas du passeport électronique n'est pas un cas isolé !

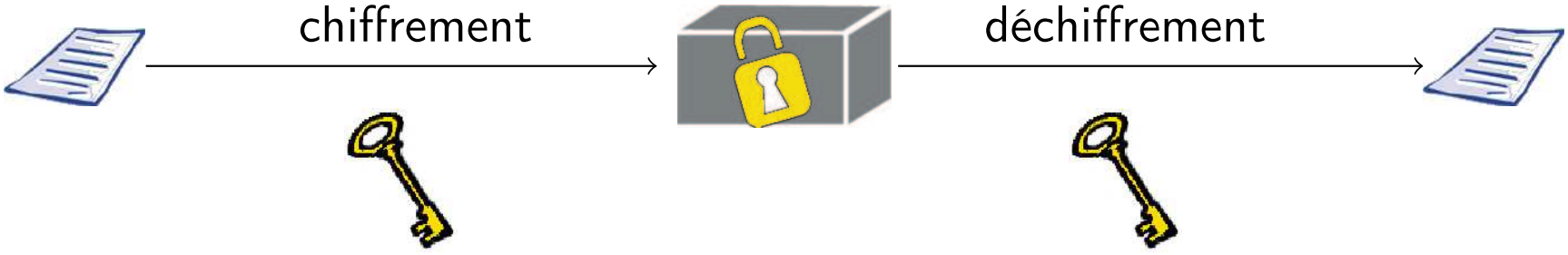
Grand format : des puces électroniques partout
JT de 20h du 4 décembre 2016 sur France 2

CNIL
Commission Nationale de l'Informatique et des Libertés

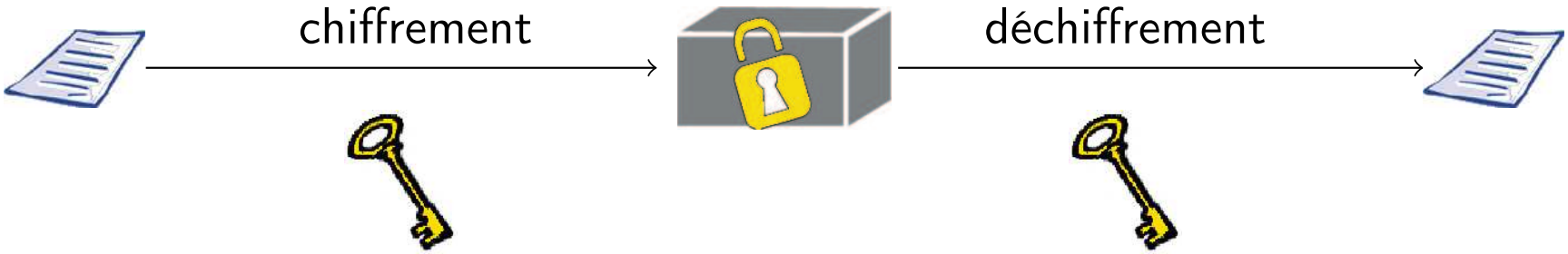
La CNIL reste préoccupée par l'accessibilité des données. Elle invite à mettre en oeuvre un chiffrement des échanges, rendant tout accès aux données impossible.

Le chiffrement : un premier rempart

Chiffrement symétrique



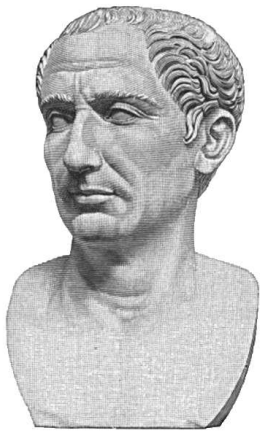
Chiffrement symétrique



Quelques exemples :

scytale (400 av. JC)

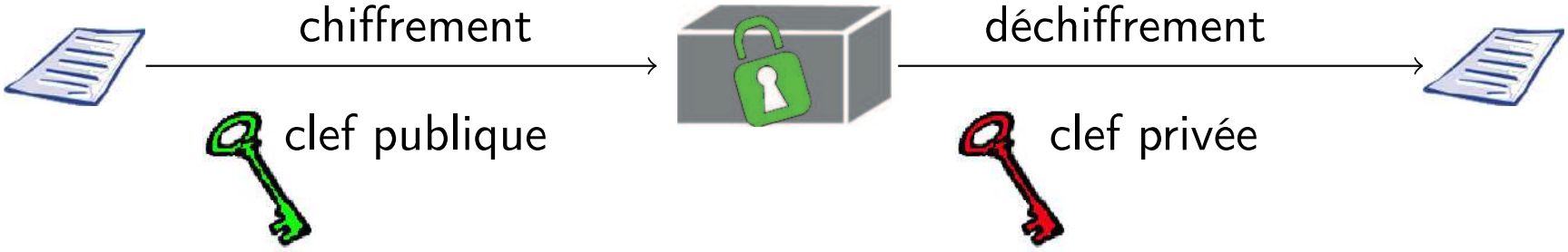
César (50 av. JC)



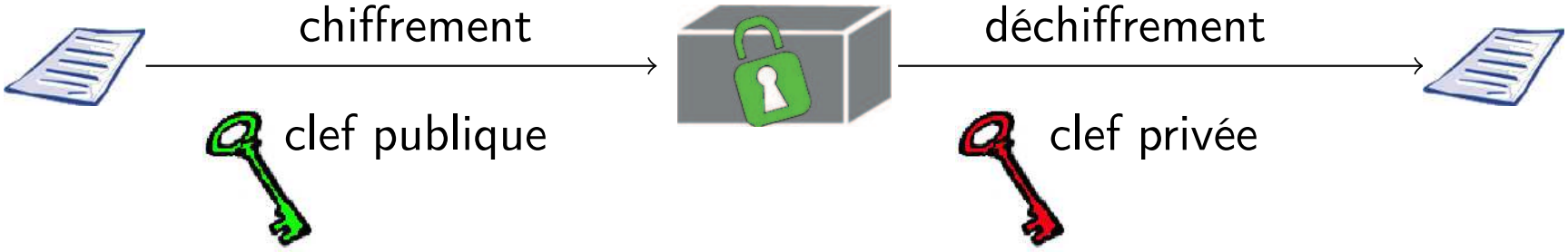
Enigma (1940)

Plus récemment, Data Encryption Standard (1977), Advanced Encryption Standard (2000).

Chiffrement asymétrique

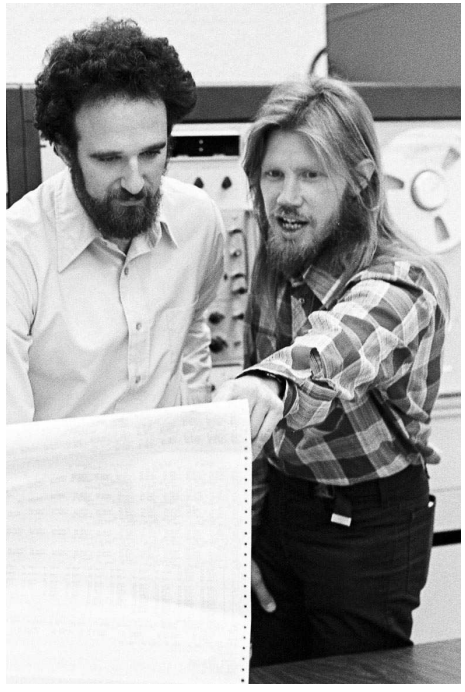


Chiffrement asymétrique



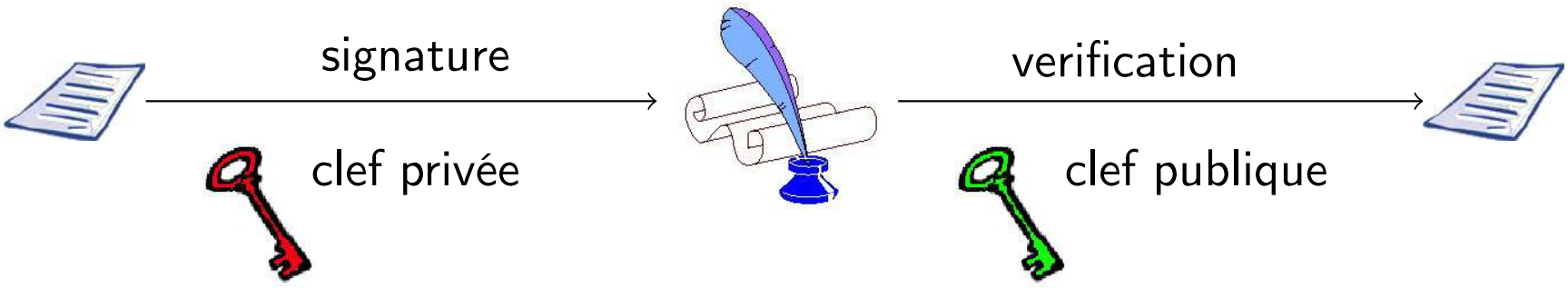
Quelques exemples :

- 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.

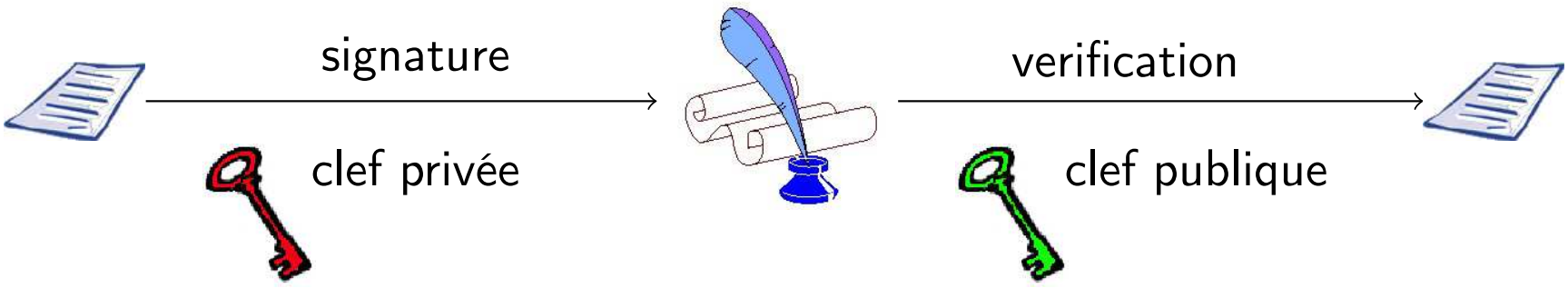
Signature



Objectifs :

- authentifier le signataire ;
- assurer l'intégrité des données signées.

Signature



Objectifs :

- authentifier le signataire ;
- assurer l'intégrité des données signées.

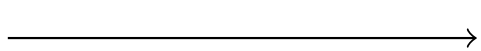
Un exemple bien connu !

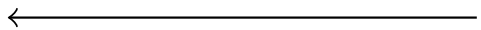
- 1997 : Affaire Serge Humpich et la fameuse « Yes card »
- À l'époque : 320 bits de clefs seulement !

Comment utiliser

ces « briques » cryptographiques ?

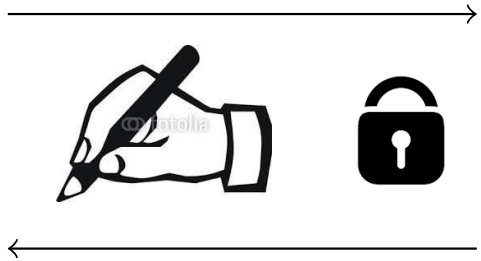
Objectif : sécuriser nos communications



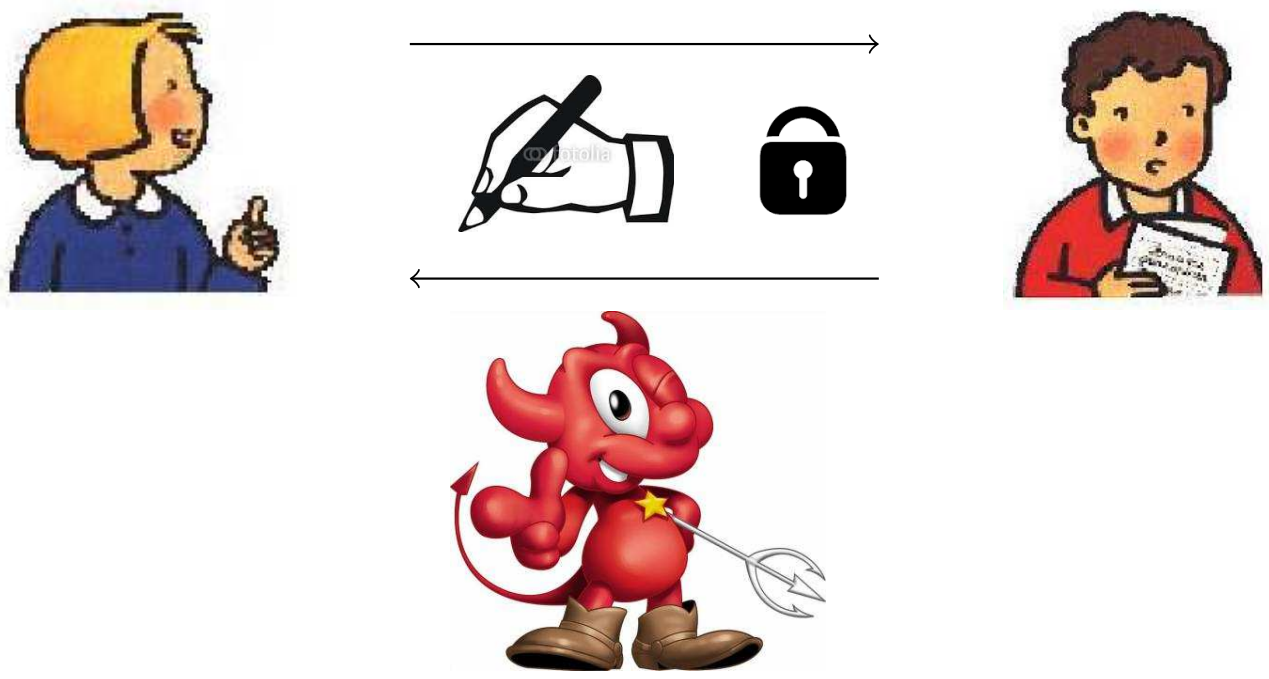


Objectif : sécuriser nos communications

Objectif : sécuriser nos communications



Objectif : sécuriser nos communications



- Cryptographie : utilisation de primitives cryptographiques (e.g. chiffrement symétrique, asymétrique, signature, . . .)
- Protocole : petit programme explicitant comment les échanges vont se dérouler

$\longrightarrow$ les protocoles cryptographiques

Passeport électronique — 2ème Génération

Le protocole BAC est un protocole d'établissement de clef qui a été mis au point pour protéger nos données personnelles, et assurer la non traçabilité des détenteurs de passeport.

Passeport émis en France à partir de 2006.

Passeport électronique — 2ème Génération

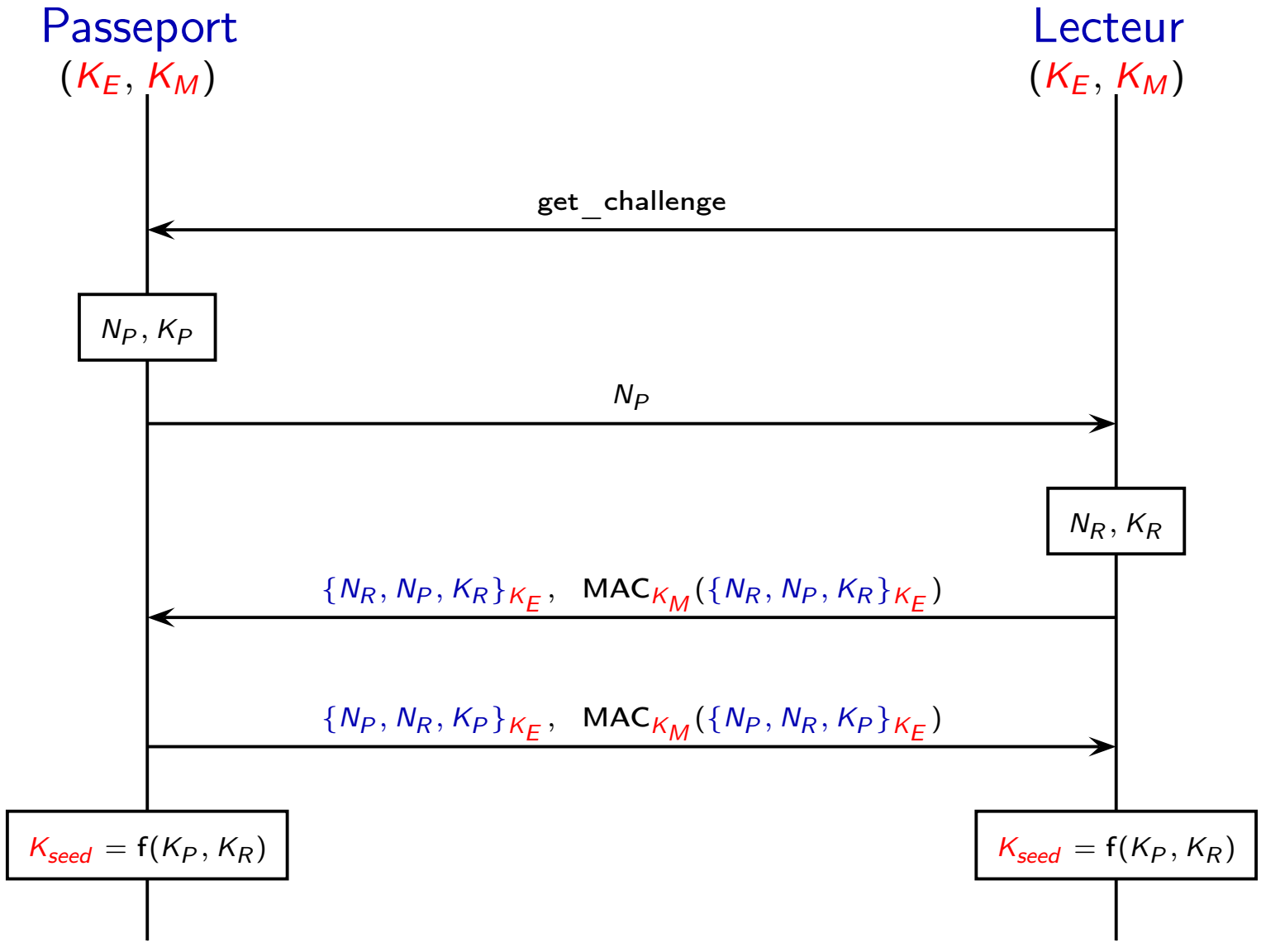
Le protocole BAC est un protocole d'établissement de clef qui a été mis au point pour protéger nos données personnelles, et assurer la non traçabilité des détenteurs de passeport.

Passeport émis en France à partir de 2006.

ISO/IEC standard 15408

Un utilisateur doit pouvoir utiliser plusieurs fois un service ou une ressource sans qu'un tiers ne puisse établir un lien entre ces différentes utilisations.

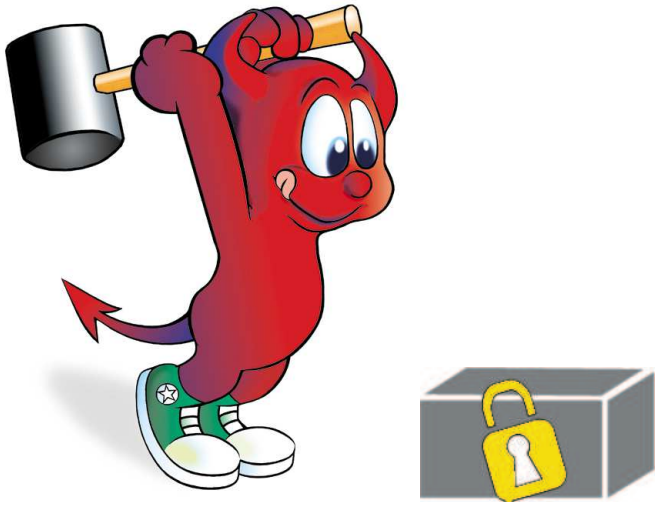
Protocole BAC



Comment peut-on attaquer ces protocoles ?

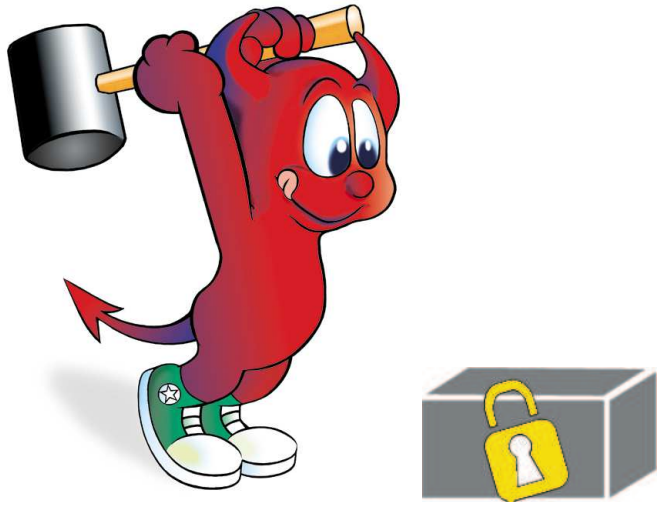
Comment peut-on attaquer ces protocoles ?

En essayant de casser
les primitives cryptographiques !



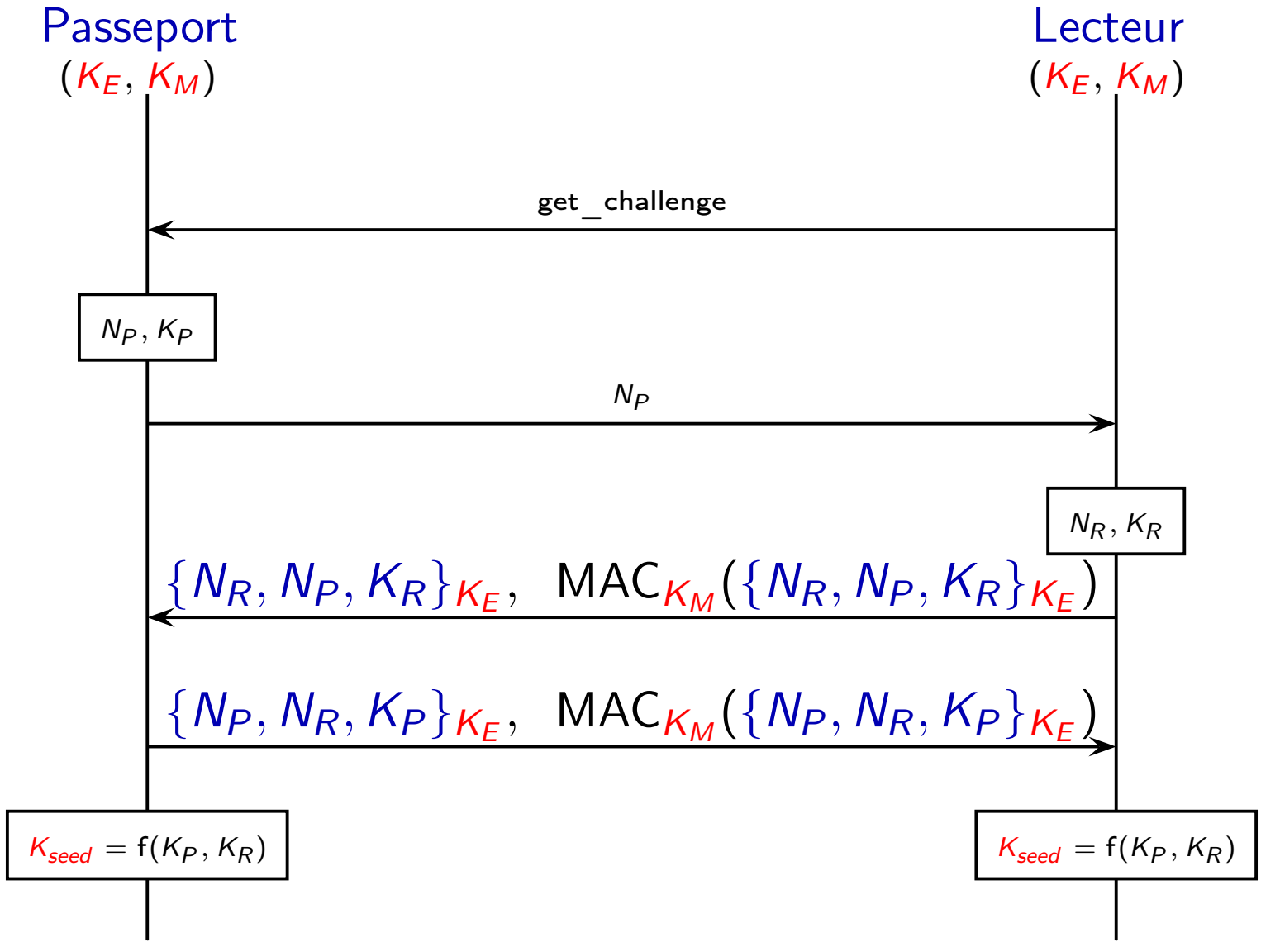
Comment peut-on attaquer ces protocoles ?

En essayant de casser
les primitives cryptographiques !



En exploitant des failles provenant d'une mauvaise conception du protocole.

Retour sur le protocole BAC



Protocole de Denning Sacco (1981)

$\longrightarrow$ version simplifiée

$$\text{aenc}(\text{sign}(k_{AB}, \text{priv}(A)), \text{pub}(B))$$

Est-ce un bon protocole d'établissement de clefs ?

Protocole de Denning Sacco (1981)

$\longrightarrow$ version simplifiée

$$\text{aenc}(\text{sign}(k_{AB}, \text{priv}(A)), \text{pub}(B)) \longrightarrow$$

Est-ce un bon protocole d'établissement de clefs ? Non !

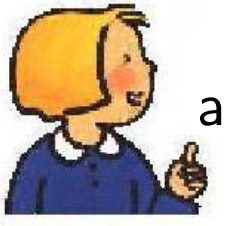
Protocole de Denning Sacco (1981)

$\longrightarrow$ version simplifiée

$$\text{aenc}(\text{sign}(k_{AB}, \text{priv}(A)), \text{pub}(B)) \longrightarrow$$

Est-ce un bon protocole d'établissement de clefs ? Non !

Description de l'attaque :



$$\text{aenc}(\text{sign}(k_{AC}, \text{priv}(A)), \text{pub}(C)) \longrightarrow$$

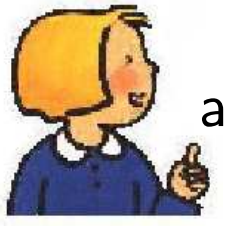
Protocole de Denning Sacco (1981)

$\longrightarrow$ version simplifiée

$$\text{aenc}(\text{sign}(k_{AB}, \text{priv}(A)), \text{pub}(B))$$

Est-ce un bon protocole d'établissement de clefs ? Non !

Description de l'attaque :



$$\text{aenc}(\text{sign}(k_{AC}, \text{priv}(A)), \text{pub}(C))$$

$\text{sign}(k_{AC}, \text{priv}(A))$

k_{AC}

$$\text{aenc}(\text{sign}(k_{AC}, \text{priv}(A)), \text{pub}(B))$$

Attaques logiques

- possible même en présence d'un chiffrement parfait,
  $\longrightarrow$ attaque par rejeu, attaque dit de « l'homme du milieu »,
  ...
- subtiles et difficiles à déceler à la simple vue de la description du protocole.

Attaques logiques

- possible même en présence d'un chiffrement parfait,
  $\longrightarrow$ attaque par rejeu, attaque dit de « l'homme du milieu », ...
- subtiles et difficiles à déceler à la simple vue de la description du protocole.

Exemple : protocole de Needham-Schroeder (1978) et sa version corrigée (1995)

$$\begin{array}{ll} A \to B : & \{A, N_a\}_{\mathrm{pub}(B)} \\ B \to A : & \{N_a, N_b\}_{\mathrm{pub}(A)} \\ A \to B : & \{N_b\}_{\mathrm{pub}(B)} \end{array} \qquad \begin{array}{ll} A \to B : & \{A, N_a\}_{\mathrm{pub}(B)} \\ B \to A : & \{B, N_a, N_b\}_{\mathrm{pub}(A)} \\ A \to B : & \{N_b\}_{\mathrm{pub}(B)} \end{array}$$

Les protocoles utilisés de nos jours ...

Google apps A. Armando et al. 2011

Possibilité d'accèder aux différents comptes (e.g. GMail, Google Calendar) d'un utilisateur.

1. créer une application malhonnête ;
2. faire en sorte que l'utilisateur y accède.

Les protocoles utilisés de nos jours ...

Google apps — A. Armando et al. 2011

Possibilité d'accèder aux différents comptes (e.g. GMail, Google Calendar) d'un utilisateur.

1. créer une application malhonnête ;
2. faire en sorte que l'utilisateur y accède.

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 toujours vulnérables

`https://freakattack.com`

Retour sur la version française du passeport

Dans la description du protocole :

- il est mentionné que le passeport doit répondre à tous les messages qu'il reçoit (éventuellement avec un message d'erreur) ;
- ces messages d'erreurs ne sont pas précisés.

Retour sur la version française du passeport

Dans la description du protocole :

- il est mentionné que le passeport doit répondre à tous les messages qu'il reçoit (éventuellement avec un message d'erreur) ;
- ces messages d'erreurs ne sont pas précisés.

Il en résulte une implémentation différente selon les nations, et ...

une attaque sur le passeport Français !

Chothia et al. 2010

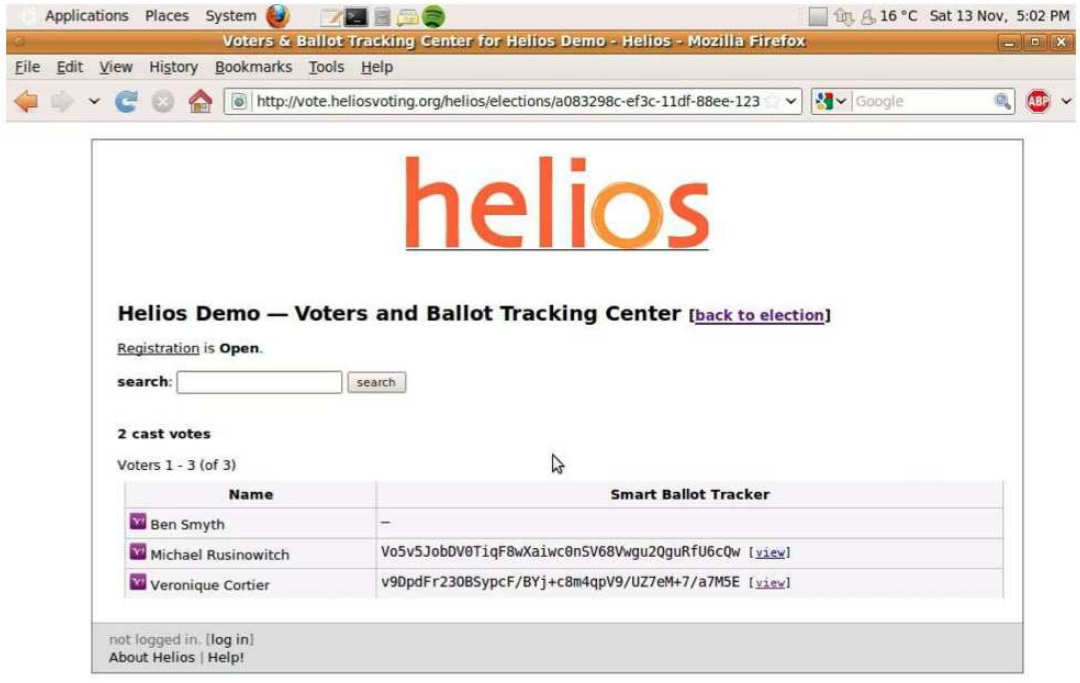
Vote électronique

Voter de façon sûre par Internet : opportunité ou illusion ?

voir l'exposé de Steve Kremer

Helios - un protocole transparent

$\longrightarrow$ développé par Ben Adida *et al.* en 2008



$\longrightarrow$ utilisé lors de plusieurs élections : à l'Université Catholique de Louvain, à l'Université de Princeton, ...

Anonymat, sans reçu, et résistance à la coercition

- Helios ne résiste pas aux formes de coercition les plus fortes
  $\longrightarrow$ il est possible d'obtenir un reçu de son vote

Anonymat, sans reçu, et résistance à la coercition

- Helios ne résiste pas aux formes de coercition les plus fortes
  $\longrightarrow$ il est possible d'obtenir un reçu de son vote
- **Helios ne satisfait même pas l'anonymat !**

Tableau d'affichage	
Alice	$\{v_A\}^{r_A}_{\mathsf{pub}(S)}$
Bob	$\{v_B\}^{r_B}_{\mathsf{pub}(S)}$

Anonymat, sans reçu, et résistance à la coercition

- Helios ne résiste pas aux formes de coercition les plus fortes
  $\longrightarrow$ il est possible d'obtenir un reçu de son vote
- **Helios ne satisfait même pas l'anonymat !**

Tableau d'affichage	
Alice	$\{v_A\}^{r_A}_{\text{pub}(S)}$
Bob	$\{v_B\}^{r_B}_{\text{pub}(S)}$

$\{v_C\}^{r_C}_{\text{pub}(S)}$ $\longleftarrow$

Anonymat, sans reçu, et résistance à la coercition

- Helios ne résiste pas aux formes de coercition les plus fortes
  $\longrightarrow$ il est possible d'obtenir un reçu de son vote
- **Helios ne satisfait même pas l'anonymat !**

Tableau d'affichage	
Alice	$\{v_A\}^{r_A}_{\mathsf{pub}(S)}$
Bob	$\{v_B\}^{r_B}_{\mathsf{pub}(S)}$
Chris	$\{v_C\}^{r_C}_{\mathsf{pub}(S)}$

Anonymat, sans reçu, et résistance à la coercition

- Helios ne résiste pas aux formes de coercition les plus fortes
  $\longrightarrow$ il est possible d'obtenir un reçu de son vote
- **Helios ne satisfait même pas l'anonymat !**

Tableau d'affichage	
Alice	$\{v_A\}^{r_A}_{\text{pub}(S)}$
Bob	$\{v_B\}^{r_B}_{\text{pub}(S)}$
Chris	$\{v_C\}^{r_C}_{\text{pub}(S)}$

Si Chris « joue » comme Alice (i.e. $\{v_C\}^{r_C}_{\text{pub}(S)} = \{v_A\}^{r_A}_{\text{pub}(S)}$) alors après publication du résultat, on pourra lever l'anonymat des participants.

Attaque découverte en 2011 par B. Smyth et V. Cortier

Que faire ?

Comment se protéger contre ces attaques ?

$\longrightarrow$ en tant que consommateur

- mettre à jour régulièrement nos logiciels ;
- s'équiper de petits étuis pour bloquer les émissions des cartes sans contact (attaque par relais)
- ...

Comment se protéger contre ces attaques ?

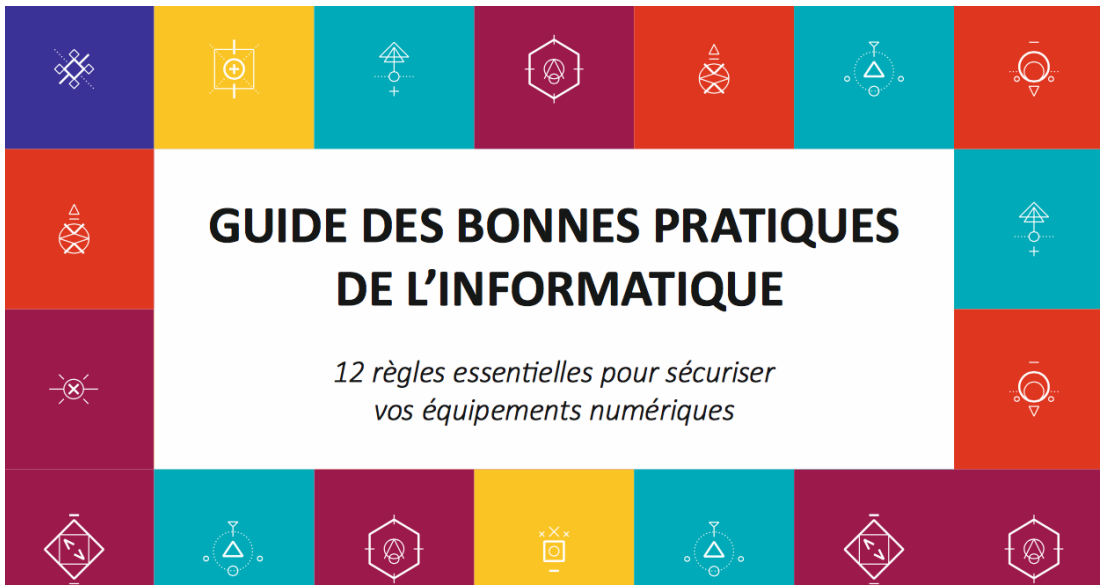
$\longrightarrow$ en tant que consommateur

- mettre à jour régulièrement nos logiciels ;
- s'équiper de petits étuis pour bloquer les émissions des cartes sans contact (attaque par relais)
- ...

Comment se protéger contre ces attaques ?

$\longrightarrow$ en tant que consommateur

- mettre à jour régulièrement nos logiciels ;
- s'équiper de petits étuis pour bloquer les émissions des cartes sans contact (attaque par relais)
- ...



$\longrightarrow$ disponible sur le site de l'ANSSI

Comment éviter ces attaques ?

$\longrightarrow$ en tant que développeur de nouvelles applications

- réserver l'invention de nouveaux protocoles aux experts du domaine ;
- préférer un protocole sur étagère sans succomber à la tentation de le simplifier ;

Comment éviter ces attaques ?

$\longrightarrow$ en tant que développeur de nouvelles applications

- réserver l'invention de nouveaux protocoles aux experts du domaine ;
- préférer un protocole sur étagère sans succomber à la tentation de le simplifier ;
- respecter quelques conseils simples lors de la conception ;

  Prudent engineering practice for cryptographic protocols
  M. Abadi et R. Needham, 1994
- prouver la sécurité (et en particulier l'absence de faille logique) avant le déploiement du protocole.

Comment éviter ces attaques ?

$\longrightarrow$ en tant que développeur de nouvelles applications

- réserver l'invention de nouveaux protocoles aux experts du domaine ;
- préférer un protocole sur étagère sans succomber à la tentation de le simplifier ;
- respecter quelques conseils simples lors de la conception ;

  Prudent engineering practice for cryptographic protocols
  M. Abadi et R. Needham, 1994
- prouver la sécurité (et en particulier l'absence de faille logique) avant le déploiement du protocole.

Peut-on prouver la sécurité des communications ?

voir l'exposé d'Hubert Comon-Lundh

À retenir

Des primitives robustes, c'est bien . . .

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

À retenir

Des primitives robustes, c'est bien . . .

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

Questions ?