

**DEA Informatique - Rennes 1 - 2001-2002**  
**SFRC**

**Sécurité des systèmes informatiques**

(Durée : 1h30)

Le vote électronique

Ludovic MÉ

janvier 2002

Nous nous intéresserons pour cet examen à un protocole de vote électronique inspiré par « A Practical Secret Voting Scheme for Large Scale Elections », de Atsushi Fujioka, Tatsuki Okamoto et Kazuo Ohta (AUSCRYPT'92).

Initialement, les électeur s'inscrivent sur une liste d'électeurs gérée par une autorité  $A$  de bi-clé ( $P_A = (e, n), S_A = (d, n)$ ). A l'inscription, on leur remet la clé publique  $P_A$  de  $A$ , un identifiant  $ID$ , un mot de passe personnel  $PSW$  et des bulletins de votes électroniques  $B_i$ .

### Exercice 1

Avant l'élection, l'électeur envoie à  $A$  :

$\{r^e H(B, Hkey)[n], ID, PSW\}_{K_{val}}$ ,  $\{H(r^e H(B, Hkey)[n], ID, PSW)\}_{K_{val}}$ ,  $\{K_{val}\}_{P_A}$   
dans lequel :

- $r$  est un nombre aléatoire généré par l'électeur,
- $H$  est un algorithme de hachage,
- $B$  est le bulletin de vote de son choix (prix parmi les  $B_i$ ),
- $Hkey$  et  $K_{val}$  sont des clés générées par l'électeur.

**Question :** Quels sont les contrôles que doit faire  $A$  à la réception de ce message? Pourquoi?

Si les contrôles sont positifs,  $A$  signe ( $r^e H(B, Hkey)[n]$ ) et envoie le résultat vers l'électeur.

**Questions :**

- Quelle est le résultat de la signature?
- Que fait le client à la réception? Pourquoi?
- Quel est le rôle de l'aléa  $r$ ?

## Exercice 2

Le jour de l'élection, l'électeur envoie au bureau de vote  $BV$  de bi-clé  $(P_{BV}, S_{BV})$  :  
 $\{H(B, Hkey)^d[n], B, Hkey\}_{K_{vote}}$ ,  $\{H(H(B, Hkey)^d[n], B, Hkey)\}_{K_{vote}}$ ,  $\{K_{vote}\}_{P_{BV}}$

**Question :** Quels contrôles le bureau de vote entreprend-t-il après réception de ce message? Pourquoi?

A l'issu de ces contrôles, le bureau de vote compte les bulletins, puis publie  $H(B, Hkey)^d[n], B, Hkey$ .

**Question :** Pourquoi cette publication? Expliquez.

## Exercice 3

Tout citoyen peut exiger qu'un système de vote électronique soit :

- Démocratique: seul les électeurs autorisés peuvent voter et il est impossible d'empêcher un électeur autorisé de voter.
- Respectueux de la vie privée : il n'est pas possible de faire le lien entre un électeur et un bulletin. En outre, il est impossible à un électeur de prouver pour qui il a voté.
- Exact : il est impossible d'altérer un bulletin ou de le détruire s'il est valide. En outre, tout bulletin valide doit être pris en compte.
- Contrôlable: chacun peut vérifier le décompte final des bulletins.

**Question :** Ces exigences sont-elles remplies par le protocole ci-dessus? Expliquez.

## Question subsidiaire

Au printemps 2002, nous aurons l'occasion de voter à plusieurs reprises. Feriez-vous confiance au protocole de vote électronique ci dessus? Justifiez votre réponse.