TD 5 : La cryptographie appliquée au vote électronique

1 Protocole de vote électronique

1.1 Déscription

Le vote électronique améliore le confort du citoyen qui peut voter de son domicile sur une période de votation plus longue tout en permettant un dépouillement quasi instantané.

Cependant, et par définition, le vote électronique dématérialise les bulletins de vote ce qui semble pouvoir permettre les escroqueries à grandes échelles. Pour un sujet aussi sensible, il convient de proposer un protocole assurant à chaque citoyen que son vote a bien été pris en compte tout en laissant celui-ci anonyme. De plus, il convient qu'aucun intervenant ne puisse introduire, modifier ou acheter des votes.

Plusieurs protocoles existent mais ceux-ci ont des idées communes qu'on va présenter à travers une vision simplifiée.

1.2 Outils :

- Cryptosystème à clé publique (RSA)
- Signatures numériques
- Fonctions de hachage
- Signatures à l'aveugle

1.3 Signature à l'aveugle

Nous allons proposer un protocole où Bob appose sa signature sur un message produit par Alice sans pour autant en connaître le contenu, comme si ce message figurait dans une enveloppe en papier qu'il lui suffit de signer pour apposer sa signature sur le document sans pour autant décacheter l'enveloppe.

Supposons que Bob ait conçu un système cryptographique RSA de clé publique (e, N) et de clé privée d. Alice souhaite voir Bob signer un message m codé sous la forme d'un entier compris entre 0 et $\mathsf{N}-1$. Alice commence par choisir un entier k premier avec N qui joue le rôle de facteur de masquage. Alice transmet ensuite à Bob, l'entier

$$m' = mk^e \pmod{\mathsf{N}}$$

Ne connaissant pas k, Bob ne peut déterminer m et ne connaît donc pas le message transmis par Alice. Bob peut néanmoins apposer sa signature au message en transmettant à Alice la valeur

$$m'' = (m')^d \pmod{\mathsf{N}}$$

À partir de cette signature masquée m'', Alice n'a alors plus qu'à évaluer

$$s = m''/k \pmod{\mathsf{N}}$$

pour disposer d'un entier s vérifiant $s^d = m \pmod{\mathsf{N}}$.

Ainsi, avec le couple (m, s), Alice dispose d'un message signé par Bob alors que celui-ci ne connaît pas la nature du message qu'il a indirectement signé.

anca.nitulescu@ens.fr

Exercice 1 Montrer que $s = m''/k \pmod{\mathsf{N}}$ est une signature RSA valide du message m.
Indication : Appliquez l'algorithme de vérification de signature RSA au couple (m, s).

Exercice 2 On considère le module RSA $\mathsf{N} = 55$ et la clé publique $\mathsf{e} = 27$.

1. Trouvez la clé privée d associé.
2. Avec un camarade jouez les roles d'Alice et de Bob dans le schéma pour signer à l'auvegle un message m de votre choix.

2 Fonctionnement

Les outils étant exposés, il ne reste plus qu'à voir comme les exploiter pour former un protocole de vote électronique.

2.1 Les intervenants

Pour organiser le scrutin, nous allons faire intervenir plusieurs entités, cela permettra en particulier de réduire le pouvoir de chacune. Ces entités apparaîtront comme étant des serveurs autonomes et indépendants communiquant entre eux de façon chiffrée. En pratique, ces serveurs seront démultipliés afin de sécuriser le système par redondance pour le cas où l'un d'eux ne réaliserait pas sa fonction.

Ces entités sont :

- **le commissaire** au vote qui servira à vérifier le droit de vote d'un citoyen ;
- **l'administrateur** qui servira à concevoir des bulletins de vote authentiques et infalsifiables ;
- **l'anonymiseur** qui réceptionnera les votes tel une urne,
- **le décompteur** qui comptera les bulletins une fois la session de vote finalisée.

L'administrateur et le décompteur disposent chacun d'un système cryptographique avec une clé publique et une clé privée.

2.2 Préparation du scrutin

A chaque électeur est envoyé une carte où figurent deux codes N_1 et N_2 générés aléatoirement. Pour fixer les idées ces codes seront formés par 12 caractères, chiffres ou lettres, ce qui propose $(10 + 26)^{12} \approx 10^{18}$ combinaisons pour chacun des codes ressemblant à celui-ci

AF15 GH25 8ZQP

Le commissaire au vote dispose de la liste de tous les codes N_1 valides. Pour une population de 1 million de citoyens, la probabilité de former au hasard un code N_1 valide est $\frac{1\ 000\ 000}{(10+26)^{12}} \approx 10^{-12}$.

À l'aide d'une fonction de hachage on transforme tous les codes N_2 valides en d'autres codes appelées leurs empreintes.

On détruit ensuite la liste des codes N_2, mais on communique au commissaire au vote la liste de leurs empreintes. Le commissaire au vote ne connaît donc pas exactement les codes N_2, ceci l'empêchera par la suite de pouvoir introduire des bulletins frauduleux.

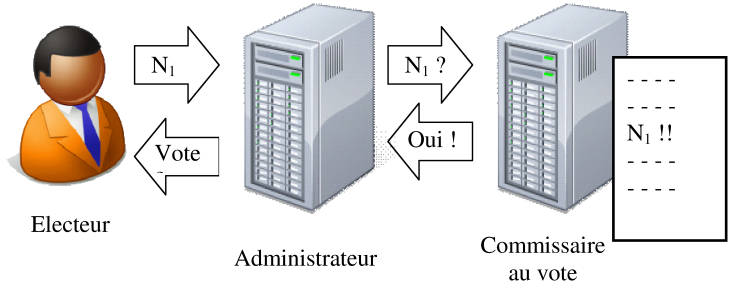
Exercice 3

1. Precisez quelle propriété de la fonction de hachage nous garantit qu'on ne peut techniquement reformer un code N_2 valide à partir de son empreinte.
2. Choisissez deux codes personnels N_1 et N_2 de 12 caractères.
3. Calculez la valeur du condensé de N_2 par la fonction TTH.
   On gardera les chiffres du N_2 et pour les lettres on utilisera l'encodage usuel de l'alphabet.

Tout est prêt, le scrutin peut commencer...

2.3 Déroulement du scrutin

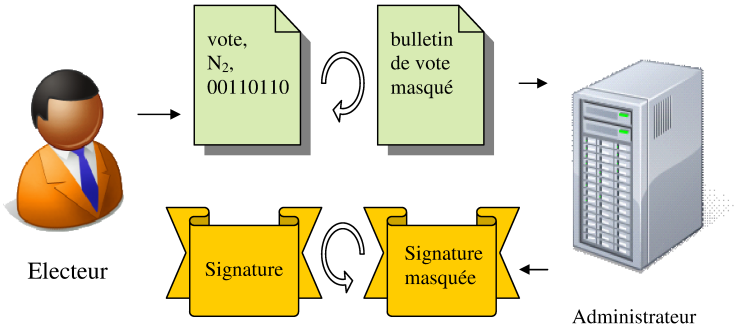
La période de votation s'ouvre. De son ordinateur et à l'aide d'un logiciel de vote officiel, l'électeur contacte l'administrateur. Il lui transmet son code N_1. L'administrateur vérifie auprès du commissaire au vote la validité du code N_1 puis, dans l'affirmative, approuve le droit de voter.



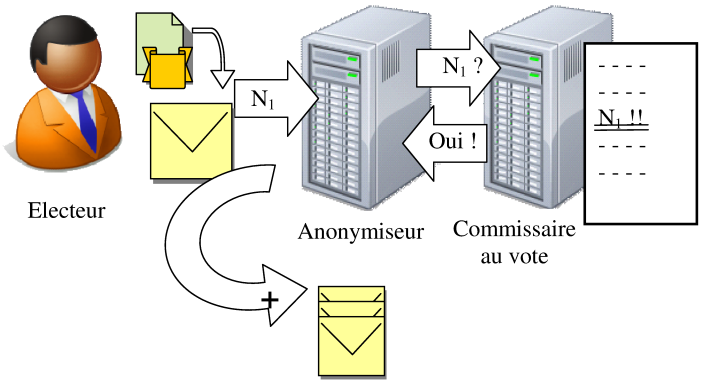
L'électeur fait son choix de vote et entre son code N_2. Le logiciel de vote forme alors un message constitué de ce vote, du code N_2 et complété par des bits aléatoires : ceci formera son bulletin de vote.

L'administrateur s'apprête à signer numériquement le vote de l'électeur. Cependant, il ne faut pas que l'administrateur ait connaissance de ce vote et c'est là que va intervenir le protocole de signature à l'aveugle.

Par un facteur de masquage, l'électeur transforme son vote et en demande la signature à l'administrateur. Une fois cette signature reçue, il retire le facteur de masquage et dispose désormais d'un bulletin de vote authentifié par l'administrateur. Il n'y a plus qu'à déposer le bulletin dans l'urne...



Le logiciel de vote contacte alors l'anonymiseur et lui envoie le code N_1 ainsi que le vote signé mais ce dernier est préalablement chiffré par la clé publique du décompteur, ce qui revient en fait à mettre le vote dans une enveloppe. L'anonymiseur vérifie auprès du commissaire que le code N_1 est valide et, dans l'affirmative, le commissaire raye le code N_1 de la liste des codes valides et l'anonymiseur enregistre le vote.



2.4 Evaluation anonyme du cours par vote

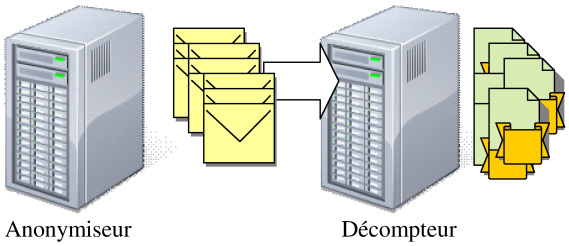
Exercice 4 En travaillant par groupes, jouez les rôles des votants, du commissaire et de l'administrateur pour organiser un scrutin qui évalue la qualité du cours de crypto.
Chaque étudiant vote en choisissant une note sur 10, qui reflète son appréciation générale du cours Cryptographie Asymétrique.

1. Distribuez vos codes N_1 et vos empreintes $TTH(N_2)$ au commissaire au vote.
2. Créez un bulletin de vote contenant la note et N_2 : $(note, N_2)$.
3. Avec les clés utilisés lors de l'exercice 2, faites la note signer à l'auvegle par l'administrateur.
4. La clé publique RSA du décompteur est $(\mathsf{e} = 3, \mathsf{N} = 583)$. Chiffrez votre vote (la note) en utilisant cette clé.
5. Envoyez votre vote chiffré avec sa signature à l'anonymisateur (votre enseignant) qui va l'enregistrer.

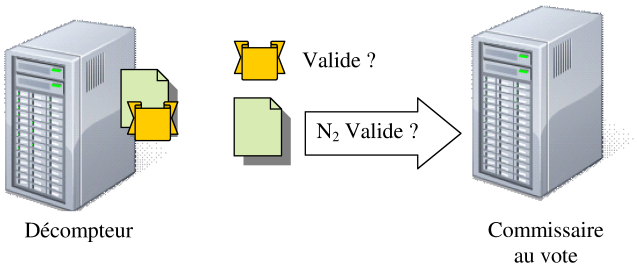
2.5 Dépouillement

La période de votation est close, l'urne est pleine il n'y a plus qu'à dépouiller, c'est le rôle du décompteur.

A l'aide de sa clé privée, le décompteur déchiffre tous les bulletins transmis par l'anonymiseur ce qui revient à retirer les bulletins de leur enveloppe.



Le décompteur réalise ensuite deux vérifications pour chaque bulletin :
- il vérifie l'authenticité de leur signature en exploitant la clé publique de l'administrateur,
- il transmet ensuite au commissaire le code N_2 figurant sur le bulletin et celui-ci calcule alors l'empreinte du code N_2 afin de vérifier que celle-ci figure dans la liste des empreintes valides.



Une fois ces vérifications effectuées, le vote est décompté.

Il est même possible de publier, les couples formés par les codes N_2 et leur vote associé ce qui permet à chacun de vérifier que son vote a bien été pris en compte.

3 Sécurité du protocole

Dans ce protocole, sans disposer du code N_1, personne ne peut usurper le droit de vote d'un citoyen. Aussi, sans disposer du code N_2, personne ne peut enregistrer un vote valide. Ainsi, ce protocole peut être considéré comme sûr au niveau des intervenants extérieurs. Il reste à vérifier que les quatre entités : administrateur, commissaire, anonymiseur et décompteur ne peuvent pas fausser la procédure.

- **Le commissaire** : Celui-ci a le pouvoir d'accepter ou de refuser des votes car c'est lui qui possède la liste des codes N_1 valides. Cependant, il n'est jamais en contact direct ni avec le votant, ni avec le vote. De plus, ne connaissant les codes N_2 que par leur empreinte, il est dans l'impossibilité de concevoir des votes valides et ne peut donc remplir l'urne.

- **L'administrateur** prend connaissance lui aussi des codes N_1 valides mais il n'a pas non plus accès aux codes N_2 ce qui l'empêche de remplir l'urne. L'administrateur est en contact avec le votant mais lorsqu'il signe son vote, il n'en connaît pas la nature car celui-ci a été préalablement masqué. De plus, il lui est à terme impossible de relier le véritable vote au votant.

- **L'anomyseur** a aussi connaissance du code N_1 mais pas du code N_2. Puisque le vote transmis est chiffré par la clé publique du décompteur, il ne connaît pas le contenu du vote. Même après le scrutin, lorsque les couples formé par N_2 et le vote associés sont publiés, il ne peut faire le lien avec un vote chiffré qui lui aurait été transmis à cause des bits aléatoires qui ont été adjoints pour former le bulletin de vote.

- **Le décompteur** a connaissance du vote mais ne peut le relier au votant. Il a aussi connaissance du code N_2 et pourrait donc transformer le vote introduit à sa guise. Cependant, la période de votation est close et l'administrateur ne signe alors plus aucun vote ce qui empêche le décompteur de concevoir un vote authentique.