République Algérienne Démocratique et Populaire

Ministère de l'Enseignement Supérieur et de la Recherche Scientifique

Université des Sciences et de la Technologie Houari Boumediene

Faculté d'Electronique et

d'Informatique Département

Informatique

Rapport de projet

Module : Cryptographie et sécurité

Thème

VOTE ÉLECTRONIQUE

Filière : Informatique

Spécialité : Sécurité des Systèmes Informatiques

Réalisé par :

- ***HAROUNI DJIHANE OUM KELTOUM***
- ***HAMDI SAMY***
- ***AIT YAHIATENE IMANE***
- ***ZIANI MOHAMED RIAD***

Travail demandé par:

Pr. A. BELKHIR

INTRODUCTION GENERALE

Avec l'avancée éminente des technologies d'information et de communication, il est possible d'automatiser toute opération jugée fastidieuse et répétitive, ce qui est le cas du vote.

Le vote électronique est une solution qui assure la confidentialité et la sécurité pour la libre expression de chaque individu et qui permet d'avoir une vue claire et globale des informations récoltées, prêtes à être exploitées.

Notre travail a pour objectif de réaliser une application qui permet l'organisation de législatives de l'an 2021 en Algérie de façon anonyme et sécurisée et automatisée. Ces mêmes résultats seront affichés à la fin du vote tout en garantissant l'authenticité et la haute disponibilité du processus.

Ce projet est composé de cinq chapitres qui sont:

➔ **Chapitre 1: Le vote électronique:**
Dans cette partie, nous présenterons les principales caractéristiques du vote électronique, ses conditions et ses avantages.

➔ **Chapitre 2: La cryptographie et la sécurisation des données dans le vote électronique:**
Dans cette partie nous définirons les différents concepts cryptographiques, des technologies et des standards utilisés pour la sécurisation des votes électroniques.

➔ **Chapitre 3:Règles du vote et de l'identification des votants:**
Dans cette partie nous parlerons des règles que nous avons adoptées afin de simuler les législatives.

➔ **Chapitre 4:La solution proposée:**
Dans cette partie nous présenterons notre solution à différents problèmes du vote électronique et nous montrerons la manière dont on a utilisé les différentes notions de sécurisation de vote dans notre plateforme web.

➔ **Chapitre 5: Environnement de travail :**
Dans cette partie nous parlerons des différents langages et outils avec lesquels nous avons implémenté notre travail

CHAPITRE 1 : Le vote électronique

1. Définition et avantages

Le vote électronique est un système de vote dématérialisé qui intègre généralement un comptage automatisé et qui est souvent réalisé à l'aide de solutions informatiques tel que les systèmes d'authentification par carte à puce, via des plateformes sur internet ou encore à distance via les bureaux de poste.

Ce système a pour but la modernisation du processus de vote et le rendre plus accessible à un plus grand nombre de personnes et

présente plusieurs avantages nous en citant quelques uns :

- Il est plus rapide d'obtenir les résultats du vote tout en évitant les erreurs de décompte.
- Il assure un meilleur respect du cadre légal des élections.
- On peut voter de chez soi, ou de n'importe où dans le monde ce qui améliore l'accessibilité au vote notamment pour les gens ayant un handicap.
- Il offre une auditabilité à l'ensemble du processus de vote en le rendant vérifiable du début à la fin.
- Il résout le problème des votes vides.
- Il permet de réduire les coûts liés à un vote physique principalement en réduisant le personnel impliqué, les divers frais de logistique et d'impression.
- En vue de la pandémie mondiale, c'est une solution que la plupart des pays envisage afin d'éviter au maximum les déplacements et les rassemblements dans des bureaux de vote.

L'un des exemples de l'adoption du vote électronique dans un contexte politique est bel et bien son intégration progressive en Suisse depuis 2003 notamment dans les votes des cantons de Genève, Neuchâtel et Zurich[1] et également lors des présidentielles aux États Unis durant l'année passée.

2. Problèmes liés au vote électronique

Le vote électronique étant une solution moderne qui permet de contrer plusieurs soucis et offrant plus de flexibilité au droit de vote des individus, il pose cependant plusieurs difficultés qui doivent être surmontées, principalement l'identification de l'électeur tout en gardant l'anonymat de son vote, la sécurisation du décompte surtout dans le cas d'un vote serré lorsque d'infimes écarts séparent les candidats et où chaque voix compte, assurer l'intégrité des votes en empêchant toute altération ou interception et enfin la solution doit assurer la confidentialité des votes en garantissant le maintien du secret des informations liées au processus de vote.

Dans le chapitre suivant nous allons introduire quelques concepts de cryptographie et de sécurisation de données utilisés dans la littérature afin de remédier aux problèmes que le vote électronique relève.

CHAPITRE 2: La cryptographie et la sécurisation des données dans le vote électronique

La sécurisation du vote électronique est présent tout au long de la chaîne de sécurité, du poste de travail du votant aux serveurs. Les données émises sont chiffrées, via un algorithme de chiffrement (RSA, Elgamal.), sur toute la chaîne de transmission. Ce chiffrement peut être établi au niveau du poste de travail, au niveau du serveur ou utiliser un double chiffrement des données. En plus de l'application des algorithmes de chiffrement il y a plusieurs technologies utilisées dans ce contexte afin d'assurer une meilleure sécurité notamment la notion de BlockChain. Dans cette partie nous allons détailler les méthodes de sécurisation et de cryptage du vote électronique.

A. Le chiffrement RSA

Le chiffrement RSA est un algorithme de cryptage asymétrique fréquemment utilisé dans le contexte de transfert de données sensibles par internet tel que le E-paiement et le E-voting afin de sécuriser ces derniers et assurer leur confidentialité et intégrité.

Les algorithmes asymétriques sont basés sur l'utilisation d'une paire de clés, une dite publique utilisée pour chiffrer et l'autre privée qui sert à déchiffrer les données. La fiabilité de cette méthode repose dans le fait qu'il est impossible pour les capacités des machines actuelles à faire les calculs nécessaires afin de casser le chiffrement par un tiers non concerné par le transfert.

Algorithme RSA

Afin d'effectuer le chiffrement RSA on suit les étapes suivantes :

1. Choisir deux nombres premiers distincts p et q ;
2. Calculer le module de chiffrement n = pq ;
3. Calculer la valeur de l'indicatrice d'Euler en n φ(n) = (p - 1)(q - 1) ;
4. Choisir un entier naturel e premier avec φ(n) et strictement inférieur à φ(n) et son inverse d, appelés respectivement exposant de chiffrement et exposant de déchiffrement ;

Si on veut chiffrer un message M on applique la formule suivante :

$$C = M^e \bmod n ;$$

Et la formule de déchiffrement est la suivante :

$$M = C^d \bmod n ;$$

B. Les signatures digitales

La signature digitale est le mécanisme qui vise à remplacer la signature manuscrite à l'aide de fonctions cryptographiques. En effet, elle permet d'établir un lien entre le document et le signataire. Ce lien peut avoir plusieurs buts, par exemple:[2]

- Identifier l'auteur d'un document.
- Marquer l'accord du signataire sur le contenu du document.
- Indiquer que le document a été lu par le signataire.
- Identifier avec certitude le signataire du document.
- Intégrité du document : on assure la non modification du document depuis qu'il a été signé.
- Non-répudiation faible du signataire : le signataire ne peut pas nier avoir signé le document. Par exemple, si un utilisateur utilise sa carte d'identité électronique pour signer électroniquement un document, il ne pourra pas par la suite nier son action.

Les cartes d'identité numériques fonctionnent avec le principe de signature digitale qui est intégrée dans ces dernières, ce qui en fait un moyen très sûr d'authentifier les votants. Le système de vote a donc l'assurance de la réalité de l'électeur, qui pourra s'exprimer une et une seule fois.

Blind signature

L'utilisation de la signature aveugle consiste à signer un document déjà masqué afin que le signataire ne puisse prendre connaissance de son contenu, ceci est fréquemment utilisé quand l'auteur et la signataire ne sont pas la même entité. C'est donc comme une enveloppe fermée qui contient un document [3].

Cette notion permet d'authentifier le votant par les autorités de vérification sans compromettre la confidentialité de son choix, c'est-à-dire que le vote sera signé par une autorité autre que celle qui chiffrera les informations du vote.

La signature aveugle utilise les mêmes algorithmes de signature que les signatures normales, la différence entre les deux réside dans l'ajout d'une couche supplémentaire de confidentialité aux documents signés.

Si on veut signer un message M on applique la formule suivante :

$$S = M^d \bmod n ;$$

Envoyer(M,S)

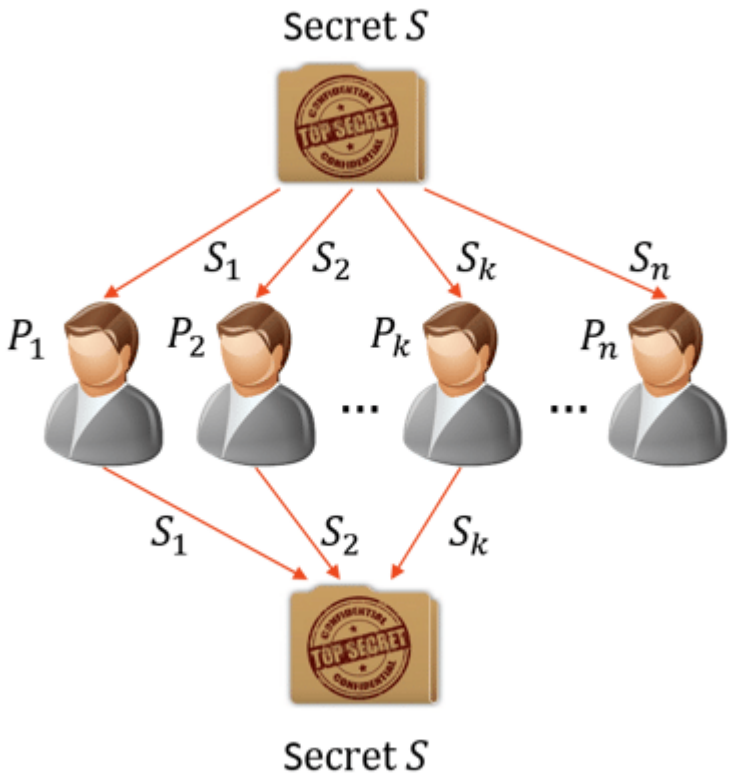
Et la formule de validation est la suivante :

$$M' = S^e \bmod n ;$$

Tester M' et M

C. Le partage de clé de Shamir

C'est un secret partagé qui est divisé en parties, donnant à chaque participant sa propre clé partagée, où certaines des parties ou l'ensemble d'entre elles sont nécessaires afin de reconstruire une phrase de passe qui donne accès au secret. Le secret de Shamir définit aussi la notion de seuil k où k représente le nombre des parties nécessaires pour reconstruire le secret d'origine[4]. La figure ci-dessous est une représentation de ce principe...



La propriété mathématique fondamentale sur laquelle le partage de clé de Shamir se repose est qu'à partir de *k* points on peut définir un polynôme de *k-1* degré, une parabole peut être définie par trois points par exemple. Cependant le choix des dis points n'est pas aléatoire car même si deux points ne définissent pas parfaitement une parabole ils décrivent son comportement, c'est pour cela qu'on doit choisir des points disjoints à l'aide de l'arithmétique des corps finis.

Dans notre système la clé de vote est partagée sur les différents partis politiques et est rassemblée au niveau du serveur par la suite.

D. Les certifications électroniques

Un certificat électronique aussi appelé certificat numérique peut être vu comme une carte d'identité numérique. Il est utilisé principalement pour identifier et authentifier une personne physique ou morale, mais aussi pour chiffrer des échanges[4]. Il contient généralement la signature d'un tiers de confiance qui atteste du lien entre l'identité physique et l'entité virtuelle certifiée. En réalité c'est un ensemble de données contenant:

- une clé publique
- des informations d'identification.
- au moins une signature construite à partir d'une clé privée, de fait quand il n'y en a qu'une, l'entité signataire est la seule autorité permettant de prêter confiance à l'exactitude des informations du certificat.

Il y a plusieurs standards de certification électronique mais le plus utilisé est le X.509 qui repose sur un chiffrement qui varie entre 40 bits et 256 bits.

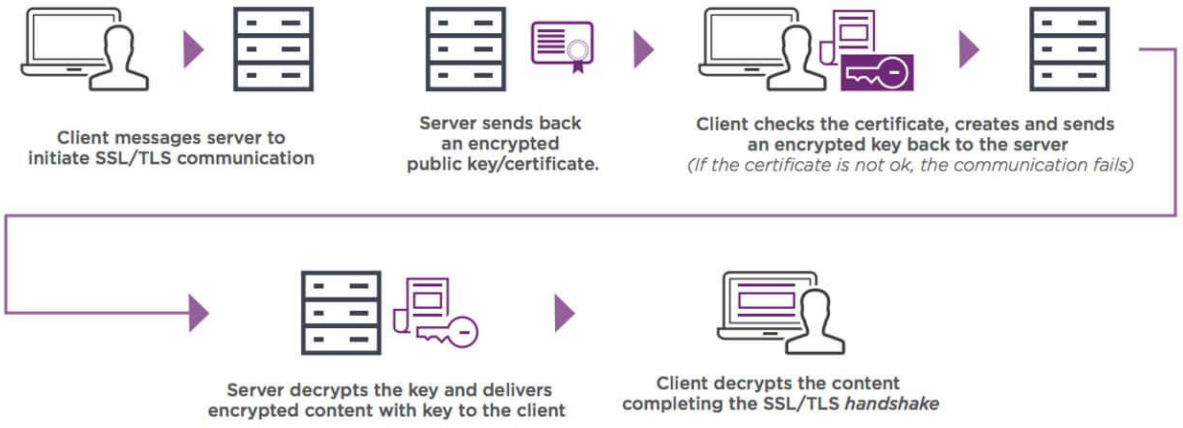
Certificat SSL

_____Le certificat numérique SSL (secure sockets layer) est un fichier de données qui lie une clé cryptographique aux informations d'une organisation. Installé sur un serveur, le certificat active le cadenas et le protocole HTTP, afin d'assurer une connexion sécurisée entre le serveur web et le navigateur. Ce certificat est utilisé surtout pour la sécurisation des transactions bancaires, du vote en ligne et toute information sensible transmise dans le web.

Le SSL lie un nom de domaine, un nom de serveur et un nom d'hôte à l'identité d'une organisation et son lieu.

Les certificats SSL utilisent la cryptographie à clé publique. La clé publique est connue par le serveur et elle est utilisée pour chiffrer n'importe quel message. Si Alice envoie un message à Bob, elle le

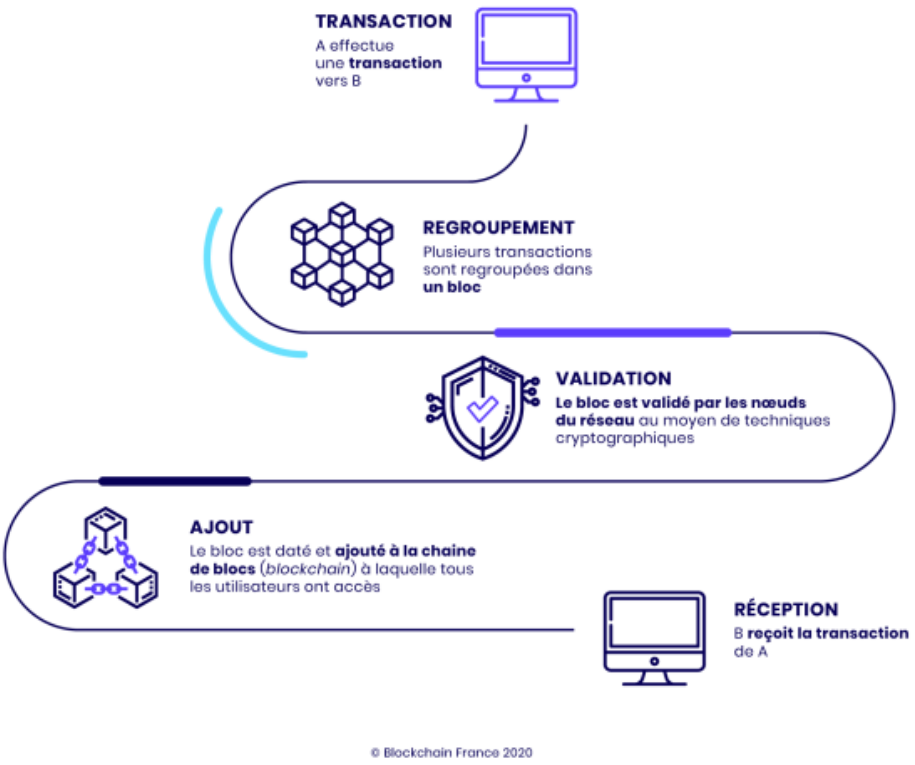
verrouille avec la clé publique de Bob, mais la seule façon de le décrypter est de le déverrouiller avec la clé privée de Bob. Bob est le seul propriétaire de sa clé privée et il est par conséquent le seul à pouvoir l'utiliser pour déverrouiller le message d'Alice. La figure suivante décrit le fonctionnement du certificat ssl .



Dans le contexte du vote électronique ce certificat ajoute une couche de protection lors de la transmission de l'information de vote depuis le navigateur web du votant jusqu'au serveur.

E. La technologie Blockchain

La Blockchain est une technologie qui permet de stocker des données numériques pour un coût minime, de manière décentralisée et sécurisée. Il s'agit d'une sorte de livre de compte qui permet de consigner et de vérifier les enregistrements qui est transparent et distribué entre les utilisateurs[7]. La figure ci-dessous montre son fonctionnement.



Cette technologie est la plus connue dans le domaine de la crypto monnaie, cependant elle a plusieurs autres utilisations notamment dans le partage de données médicales sensibles, le monitoring des systèmes IoT, les systèmes de suivi contre le blanchiment d'argent ou encore le vote électronique. En effet, le fonctionnement du blockchain fait que son utilisation dans le vote électronique permet de contrer les challenges les plus persistants de ce dernier, nous parlons ici de l'authentification, l'intégrité des données, la transparence du vote et sa vérifiabilité. Le vote électronique basé sur la blockchain permet aux électeurs de détenir une copie de l'enregistrement du vote ce qui veut dire que l'historique ne peut pas être modifié et donc il est impossible d'ajouter des votes illégitimes.[6]

L'un des concepts les plus importants dans la Blockchain est le Smart Contrat. Il s'agit de programmes autonomes qui exécutent automatiquement les conditions et termes d'un contrat, sans nécessiter d'intervention humaine une fois démarrés. Ce qui rend les transactions faites entre utilisateurs infalsifiables.

La blockchain Ethereum est souvent utilisée dans le contexte du vote électronique car elle permet de générer des comptes avec une clé publique et une clé privée qui seront utilisées dans l'architecture du bloc. Le langage Solidity est utilisé pour la création des smart contrats.

F. Vérifiabilité du vote

Le principe de vérifiabilité du vote sur Internet est un des critères permettant de s'assurer de la sécurisation des bulletins de vote : il permet aux votants de vérifier que le contenu de leur bulletin n'ait pas été modifié par un acte malveillant de type cyber attaque. D'après le cryptographe Pierrick Gaudry: "Le lien que l'on a beaucoup de mal à couper se situe entre l'identité du votant et son bulletin chiffré. Cette propriété est assurée principalement par l'intégration de la notion de blind signature dont on a parlé dans la partie 3.B et par l'utilisation de la blockchain dans le crypto-système.

G. Salage et hachage de données

Hachage

Le hachage est la transformation d'une chaîne de caractères en valeur ou en clé de longueur fixe, généralement plus courte, représentant la chaîne d'origine. Le hachage est notamment employé pour indexer et récupérer les éléments d'une base de données. Il est en effet plus rapide de trouver l'élément d'après la clé de hachage réduite plutôt qu'à l'aide de la valeur d'origine.

Cette fonction est également utilisée dans de nombreux algorithmes de chiffrement tel que le Message digest 5 dit MD5.

Salage

Le salage, est une méthode permettant de renforcer la sécurité des informations avant de les hacher (par exemple des mots de passe), elle consiste à concaténer le mot de passe avec une chaîne de caractère aléatoire.Le but du salage est de lutter

contre les attaques par analyse fréquentielle, les attaques utilisant des rainbow tables, les attaques par dictionnaire et les attaques par force brute. Pour ces deux dernières attaques, le salage est efficace quand le sel utilisé n'est pas connu de l'attaquant ou lorsque l'attaque vise un nombre important de données hachées toutes salées différemment.

CHAPITRE 3: Règles du vote et de l’identification des votants

Afin de simuler correctement un vote électronique et de mettre en évidence la partie de sécurisation et de cryptage de ce dernier nous nous sommes basés sur les règles suivantes dans notre travail:

- Les candidats du vote sont divisés par listes et chaque liste est composée au maximum de quatre individus.
- Un votant doit choisir trois candidats au total.
- Un votant peut choisir ces candidats de toutes les listes confondues, c'est-à-dire que le choix se fait selon les individus.
- Les gagnants aux élections sont les trois premier candidats ayant eu le plus grand nombre de votes.

Nous avons également réfléchi sur la meilleure façon d’identifier les votants éligibles et d‘être aussi proches de la réalité que possible nous sommes arrivés à cette idée : une base de données est préalablement conçue par les autorités légitimes selon les critères qu’ils ont prévu (âge, nationalité, etc..). Cette base de données est ensuite utilisée pour la confirmation des votants qui vont s'inscrire sur notre plateforme. Ceci garantit que seules les personnes autorisées auront le droit de voter.

CHAPITRE 4: La solution proposée

1. Choix de la plateforme de vote

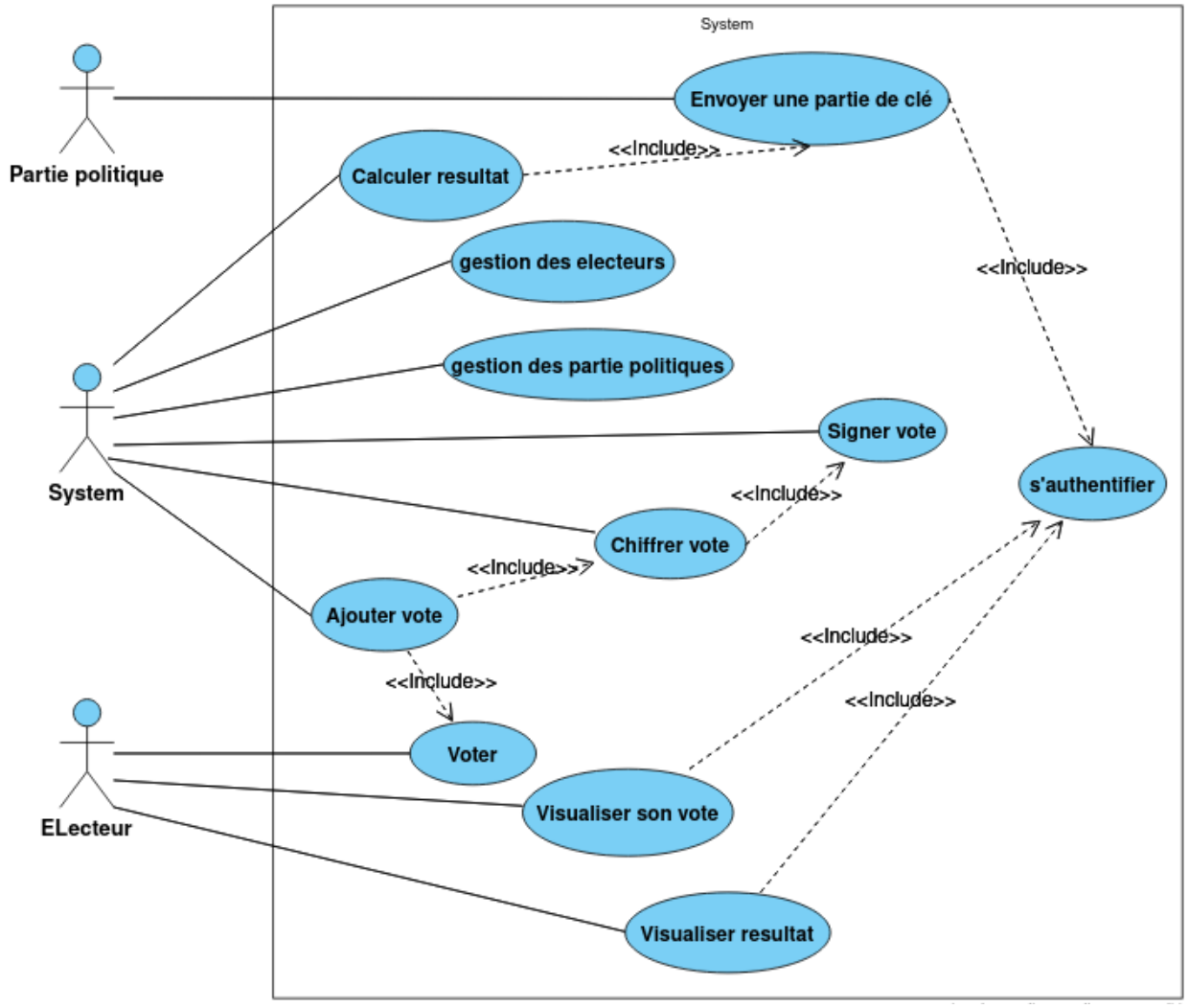
Pour ce projet nous avons concrétisé nos recherches et nos connaissances acquises en cours durant ce semestre dans le contexte du vote électronique par un site web pour les raisons suivantes :

- C'est une technologie adaptative qui est facile à manipuler.
- Il est présent sur internet ce qui le rend plus convivial et accessible par une audience plus large que si le vote se faisait dans les locaux fixes.
- Les sites web sont adaptatifs et présentent des avantages de facilité de changement de l'interface selon les besoins changeants et évoluants des utilisateurs.
- L'utilisation de sites web est un standard mondial ce qui veut dire qu'il y a plusieurs protocoles et mécanismes de bon fonctionnement et de sécurisation déjà préétablies.
- Son fonctionnement est intuitif pour tous les utilisateurs car tout le monde a l'habitude avec les sites web maintenant.

En plus de tous ces avantages nous avons éliminé les autres options à cause du manque de matériels pour concevoir un système de carte à puce, et à cause du fait qu'une application desktop n'est pas intéressante car l'installation d'un nouvel exécutable pour une action faite qu'une seule fois est suffisant pour décourager l'utilisateur du vote.

2. Conception et structure du site

a. Diagramme de cas dutilisation



Électeur

Il peut voter : choisir 3 candidats de toute la liste
après le vote il pourra consulter son vote de même il a la possibilité de visualiser les résultats après la fin du vote.

Partie politique:

Ils ont un seul rôle qui est l'envoie de la partie de la clé de décryptage qu'ils détiennent afin de pouvoir déchiffrer les votes tout en assurant confidentialité des données .

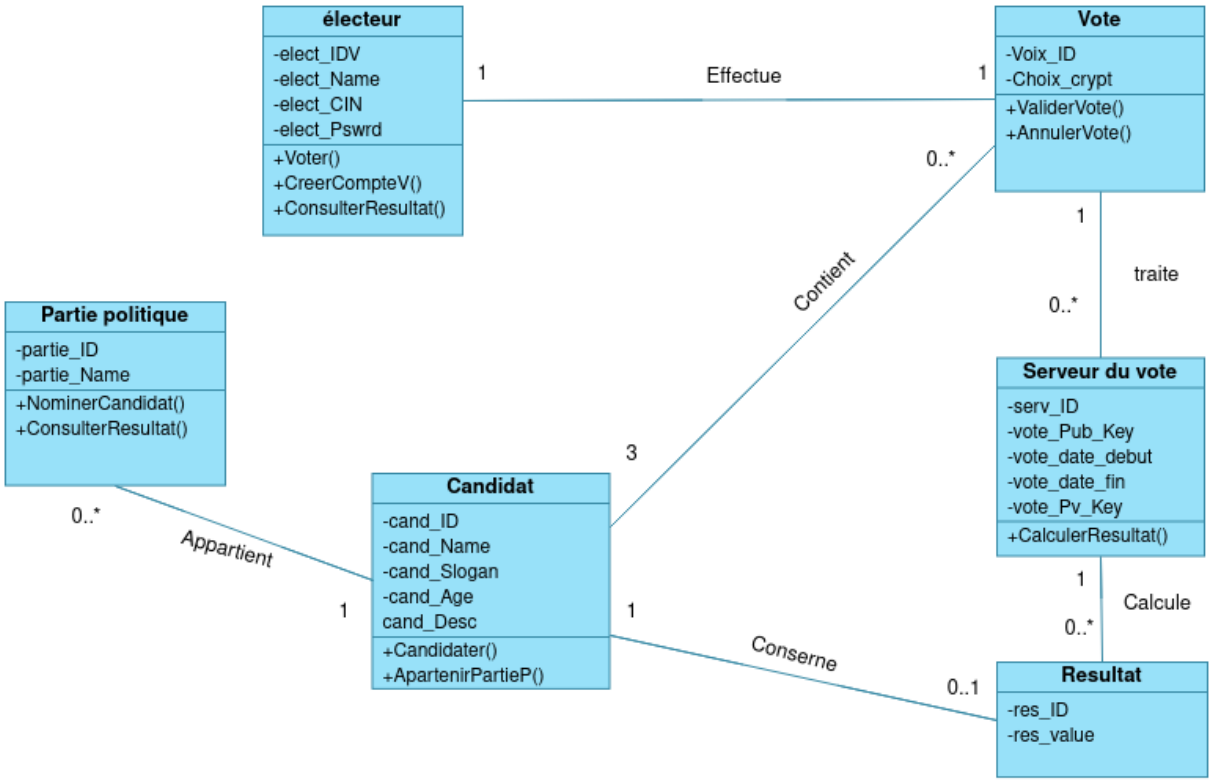
Le système ou le serveur :

Il est chargé de la gestion des parties politiques et des électeurs (ajouter ,vérifier la validité, modifier supprimer)

le serveur joue le role de la trierse personne a qui on fait confiance qui se charge de signer les vote a blanc pour garder lanonymat apres les avoir crypter afin d'assurer confidentialite des votes et enfin lenregistrer dans la base de donnes

A la fin du vote après la récupération de la clé de décryptage il calcule le nombre de vote pour chaque candidat et donc détermine les gagnants et les ajoute à la base de données.

b. Diagramme de classe



3. Sécurisation du vote

Le vote nécessite une sécurisation des données élevée et fiable c'est pour cela que nous avons conçu plusieurs couches de sécurité décrites dans les paragraphes ci-dessous, on note qu'on a utilisé le chiffrement RSA pour le cryptage et la signature des données.

Tout d'abord l'authentification d'un votant se fait selon son numéro d'identité nationale sauvegardé préalablement dans la base de données ainsi que son mot de passe haché et salé.

Lorsqu'un votant valide son choix on le crypte avant de l'envoyer au serveur en utilisant la clé publique de ce dernier, pour ensuite ajouter la couche de cryptage du certificat SSL.

Chaque voie est signée avec le principe de la blind signature qu'on a défini dans la partie 3, c'est-à-dire que les voies sont signées par un tiers de confiance qui est l'admin dans notre cas, il signe la voie avec sa clé privée et il l'envoie au serveur. Ceci garantit l'anonymat du vote.

A l'arrivée de la donnée du vote au niveau du serveur, il décrypte la couche du certificat SSL, puis vérifie la signature pour ensuite sauvegarder l'information dans la base de données tout en la gardant chiffrée.

L'algorithme de partage de clés de Shamir divise la clé secrète du serveur sur les groupes de candidats, et elle n'est rassemblée qu'à la fin du vote afin de décrypter les voies stockées dans la base de données et pour faire le calcul.

On note aussi que tous les mots de passe sont sauvegardés en hashé dans la base de données ce qui veut dire que seul l'utilisateur pourra connaître son mot de passe.

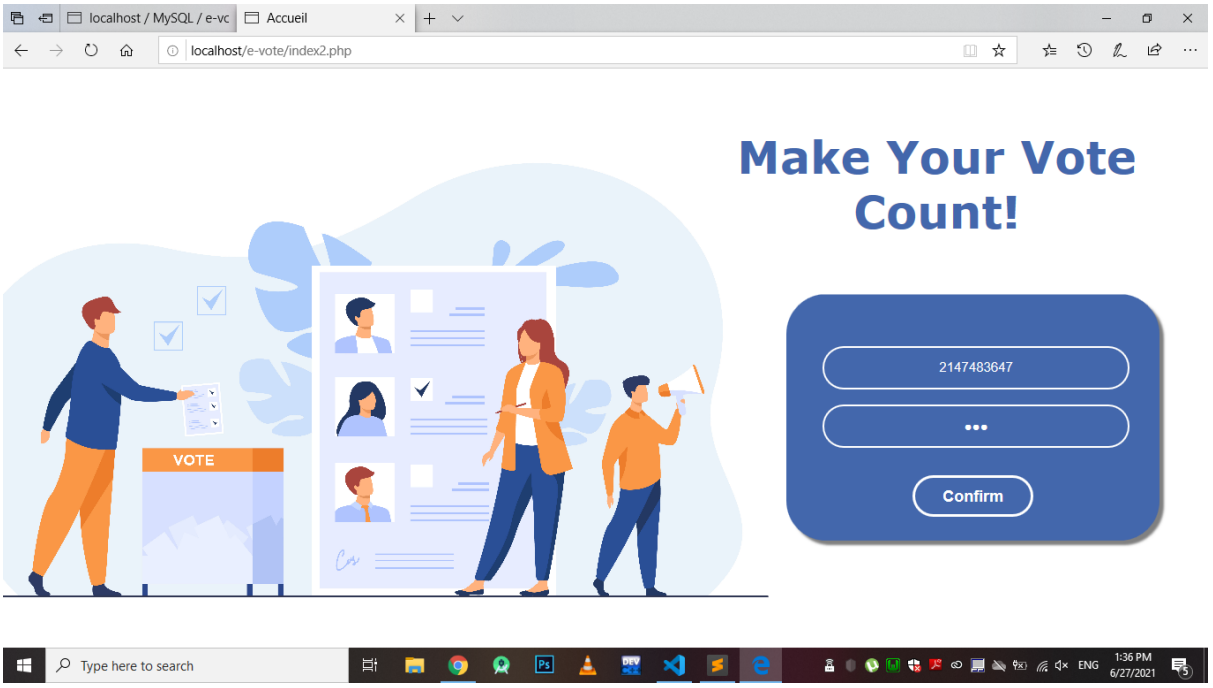
Après avoir désigné les vainqueurs au niveau du serveur on l'envoie au client cryptée via le protocole SSL.

Remarque : faute de temps et de puissance de calculs nous n'avons pas pu implémenter la notion de blockchain dans notre projet.

4. Captures d'écrans :

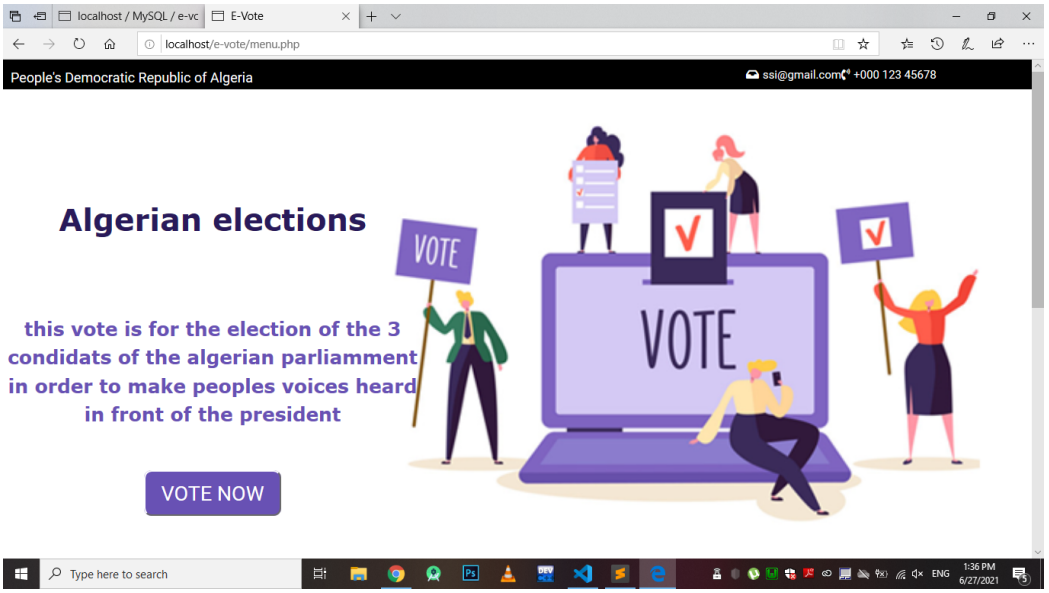
1- interface de connexion :

L'électeur doit entrer un token valide qui lui a été attribué après avoir vérifié sa ligibilité pour voter avec le mode de passe qui est hasher puis encoder a base64 pour une authentification sécurisée.

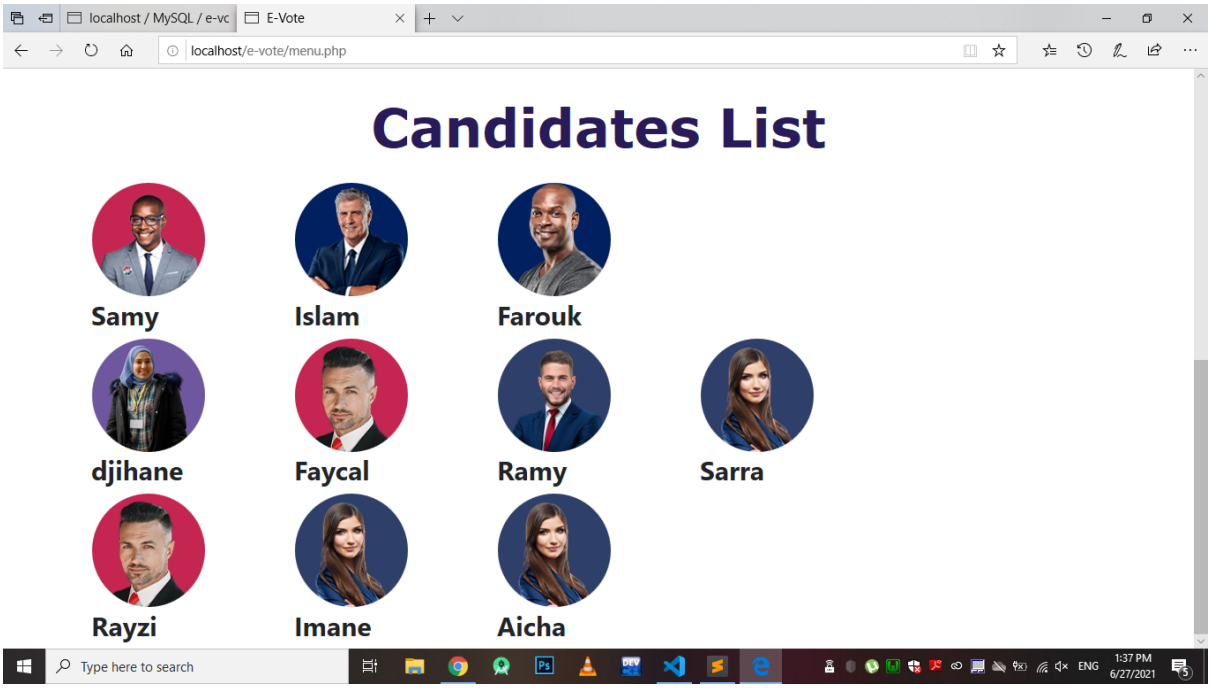


2- Interface du menu :

Après une authentification réussie ,si l'utilisateur n'a pas encore voté il sera redirectionné vers la page de menu ou il retrouve tout les listes des candidats et un bouton votez pour accéder à l'interface de vote .



La liste de tous les candidats

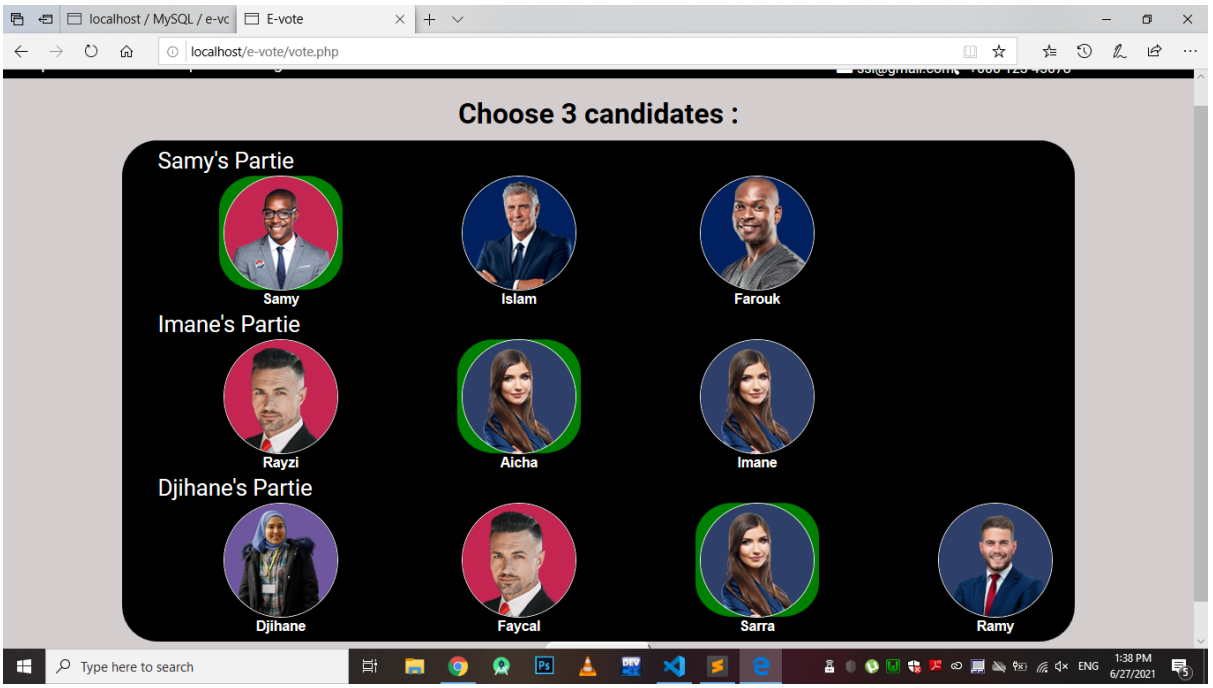


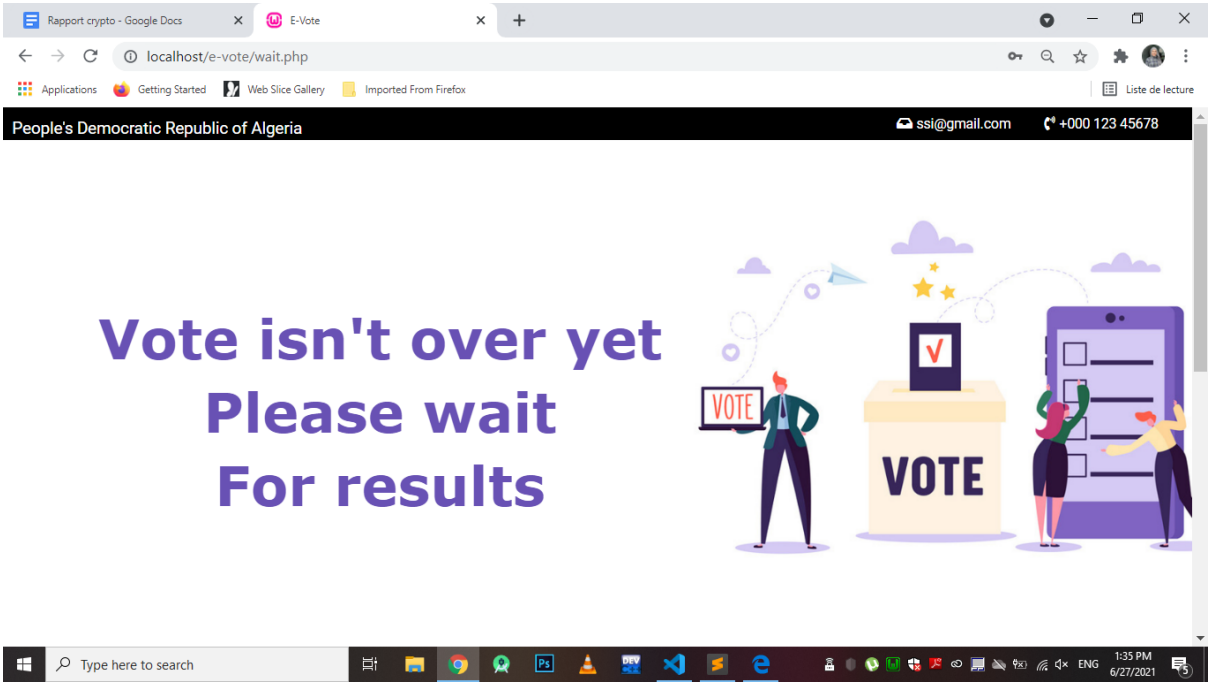
3- Interface de vote :

Dans l'interface de vote on retrouve les candidats de chaque partie politique et l'électeur doit choisir 3 candidats sinon un message s'affiche dans le cas contraire .

Le cryptage et la signature va se faire en arrière plan et le vote sera stocké dans la base de données et l'électeur sera redirectionné vers l'interface d'attente de résultat .

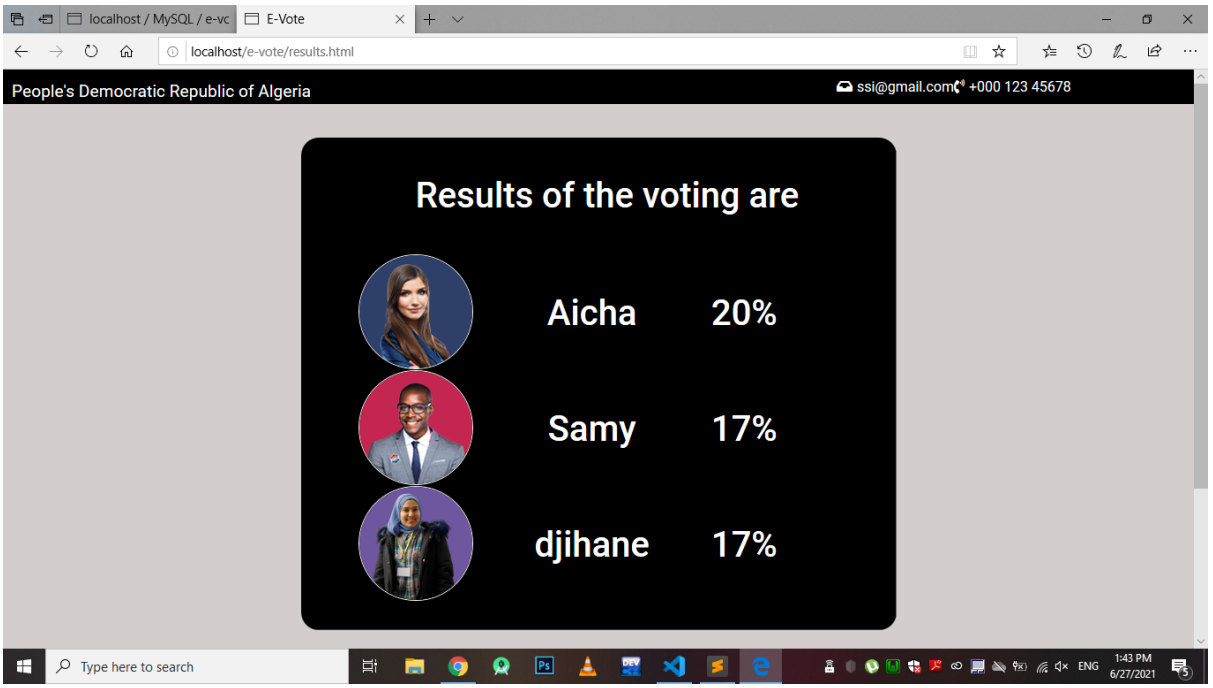
Par contre dans l'autre cas où l'électeur a déjà voté il se retrouvera dans une interface ou il pourra visualiser soit son vote ou bien consulter
les résultats si le vote est terminé.





4- Interface des résultats :

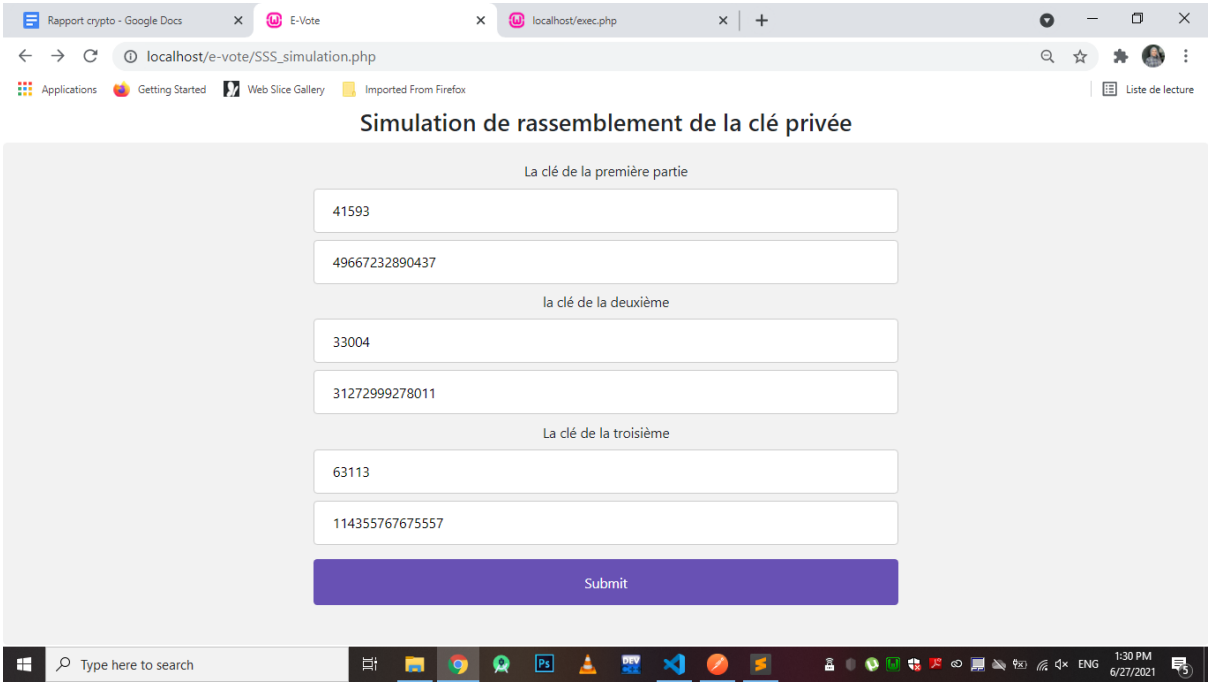
A la fin du vote on rassemble la clé de déchiffrement des parties politiques et le serveur calcule les votes et va stocker les 3 candidats gagnants dans la base de données et les affichera dans l'interface de résultat qui deviendra accessible pour tout le monde.



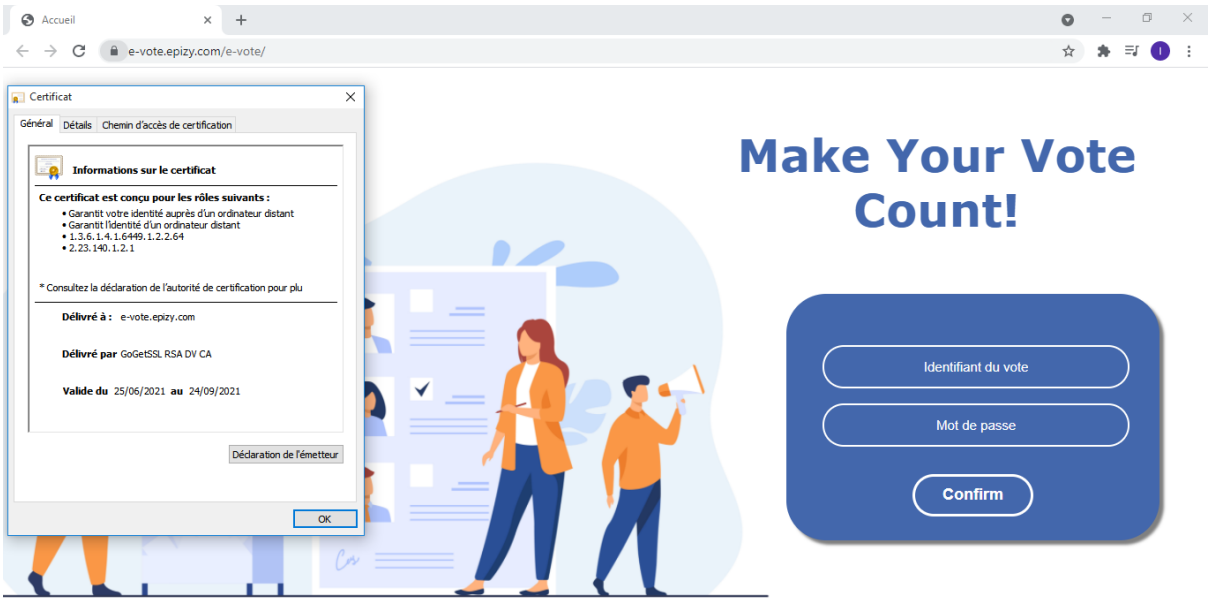
5- Interface qui simule le rassemblement de la cle privées :

Au vu du temps limité qu'on avait on a pas pu développer les comptes speciaux pour chaque partie politique ou elle recevra sa partie de la clé privée et quand le temps du trie arrive chaque partie politique entre, c'est parti de la clé et la clé sera rassemblé dans le serveur qui effectuera la catégorisation des voix et donne les résultats des candidats gagnants avec leur pourcentage.

Pour une simulation on a créé une seule interface et on a fait entre les 3 parties de la clé de décryptage des 3 parties politiques et le serveur effectue la catégorisation et enregistre les résultats dans la base de données.



6- Certificat SSL:



CHAPITRE 5: Environnement de travail

1- langages utilisés :

HTML et CSS

HTML représente la structure d'une page Web et est utilisé en conjonction avec la feuille de style en cascade (CSS) qui permet de décrire la présentation d'un document et les langages de script tels que Javascript. Il s'agit du langage de balisage hypertexte, le type standard de documents conçus pour être affichés sur le web[9].

Javascript

C'est un langage de programmation interprété de haut niveau, également abrégé en JS. Il prend en charge différents paradigmes de programmation tels que l'orienté objet, la programmation fonctionnelles ou encore la programmation prototypale. Il est principalement utilisé sur le web[10].

PHP

Hypertext Preprocessor, plus connu sous son sigle PHP, est un langage de programmation libre, principalement utilisé pour produire des pages Web dynamiques via un serveur HTTP, mais pouvant également fonctionner comme n'importe quel langage interprété de façon locale. C'est un langage impératif orienté objet. Il est considéré comme une des bases de la création de sites web dits dynamiques mais également des applications web[11].

SQL

C'est un langage de requête structurée qui sert à effectuer des opérations sur des bases de
données. Parmi ces opérations nous pouvons citer : l'ajout, la modification et la suppression de
données dans la base de données, et c'est le langage utilisé par les SGBDR tel que Oracle, MySql,Posgresql .

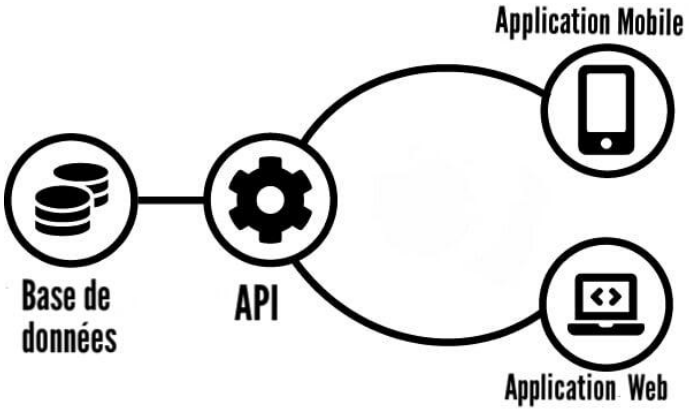
Pour ce projet on a opté pour le SGBDR **Mysql**

RESTful CRUD API :

• **API** : Signifie Application Programming Interface, est un ensemble normalisé de classes,
de méthodes, de fonctions et de constantes qui permet à deux logiciels de communiquer
entre eux. Fondamentalement, une API spécifie comment les composants logiciels doivent
interagir. Il existe plusieurs types d'API (public, partenaire, privée), dans notre cas on
a créé une API qui fait communiquer notre base de données avec notre application mobile
et notre site Web.

• **REST** : Signifie REpresentational State Transfer, Cela signifie que lorsqu'une API RESTful
est appelée, le server transfère au client une représentation de l'état de la ressource
demandée. La représentation de l'état peut être au format XML, HTML ou JSON. Pour que
qu'une API soit RESTful, elle doit suivre un ensemble de contraintes lors de sa conception.
L'ensemble de contraintes REST rendra l'API plus facile à utiliser et à découvrir.

• **CRUD** : C'est l'acronyme de Create, Read, Update, Delete. Ceux-ci forment les commandes
de base des bases de données standards. Chaque API est appelée en émettant une méthode
de requête HTTP standard : GET pour recevoir, POST pour envoyer, PUT pour modifier et
DELETE pour supprimer.



2- Outils logiciels

1- WAMPServer : C'est une plateforme de développement Web de type WAMP, permettant de faire
fonctionner localement des scripts PHP. En soi ce n'est pas un logiciel mais un environnement
comprenant deux serveurs (Apache et MySQL), un interpréteur de script (PHP), ainsi que
phpMyAdmin pour l'administration Web des bases de donées MySQL.

2- MySQL Server : C'est un système de gestion de base de données relationnelle (SGBDR) libre et
Open Source qui utilise SQL comme langage de requête structurée. Il est utilisé par de nombreux
sites Web populaires dont Facebook, Youtube, Twitter et bien d'autres [15].

3- Visual Paradigm : C'est un outil de modélisation UML, il dispose d'un éditeur UML simple,
intuitif et puissant, ce qui permet de créer des diagrammes UML professionnels précis et rapide.
On l'a utilisé pour tous nos diagrammes dans le chapitre « Analyse et Conception ».

4- Visual Studio code: C'est un éditeur de texte open source moderne qui facilite la conception d'applications Web.

5- Adobe Photoshop : C'est un logiciel très utilisé pour l'édition d'images, l'animation, la conception graphique et l'art numérique. On l'a utilisé pour créer et modifier quelques illustrations.

Conclusion

L’objectif majeur de ce projet était de concevoir une solution permettant d’adopter le vote électronique aux législatives algériennes de l’an 2021.

Initialement nous avons parlé du vote électronique et de ses avantages. Ensuite nous avons défini les différentes notions de sécurisation de vote ainsi que la technologie blockchain et les règles de simulation de notre vote. Enfin nous avons présenté notre plateforme web de vote électronique de la conception au captures d'écran afin de montrer concrètement notre implémentation.

Ce projet nous a permis d’appliquer les notions que nous avons appris au long du semestre dans un contexte réel et nous a permis de comprendre les limites de chaque élément de notre crypto-système notamment la lenteur de l’algorithme de chiffrement RSA qu’on aurait pu remplacé par un cryptage par courbe elliptique ce qui aurait amélioré les temps de calcul, et aussi d'intégrer un système d’authentification en utilisant les composants electronique Arduino. Nous avons aussi pu trouver une solution des plus modernes dans la littérature traitant le problème de vérifiabilité de d’anonymisation totale du vote: la blockchain. Nous aurions aimé l'implémenter mais le délai de remise du projet fut très court.

Malgré cela, ce travail reste une base solide qui peut se voir améliorée en vue d’une éventuelle implémentation dans un système réel, offrant plus de fonctionnalités et utilisant de meilleurs outils.

Bibliographie

1- Étude de législation comparée n° 176 - septembre 2007 - Le vote électronique

2- Signature digitale : À propos de la signature digitale - Qu'est-ce que la signature digitale ? - Sécurité Sociale

3- Secure E-Voting With A Blind Signature
4- Electronic signature and electronic certificate | UOC Library
5-Transport Layer Security — Wikipédia
6-Blockchain et vote électronique
7- What if blockchain technology revolutionised voting?
8- A Πt,nч multi-secret sharing scheme
9- HTML & CSS Courses & Tutorials
10-What is JavaScript? - Learn web development | MDN
11-PHP: Hypertext Preprocessor