Rapport sur le générateur de diplômes

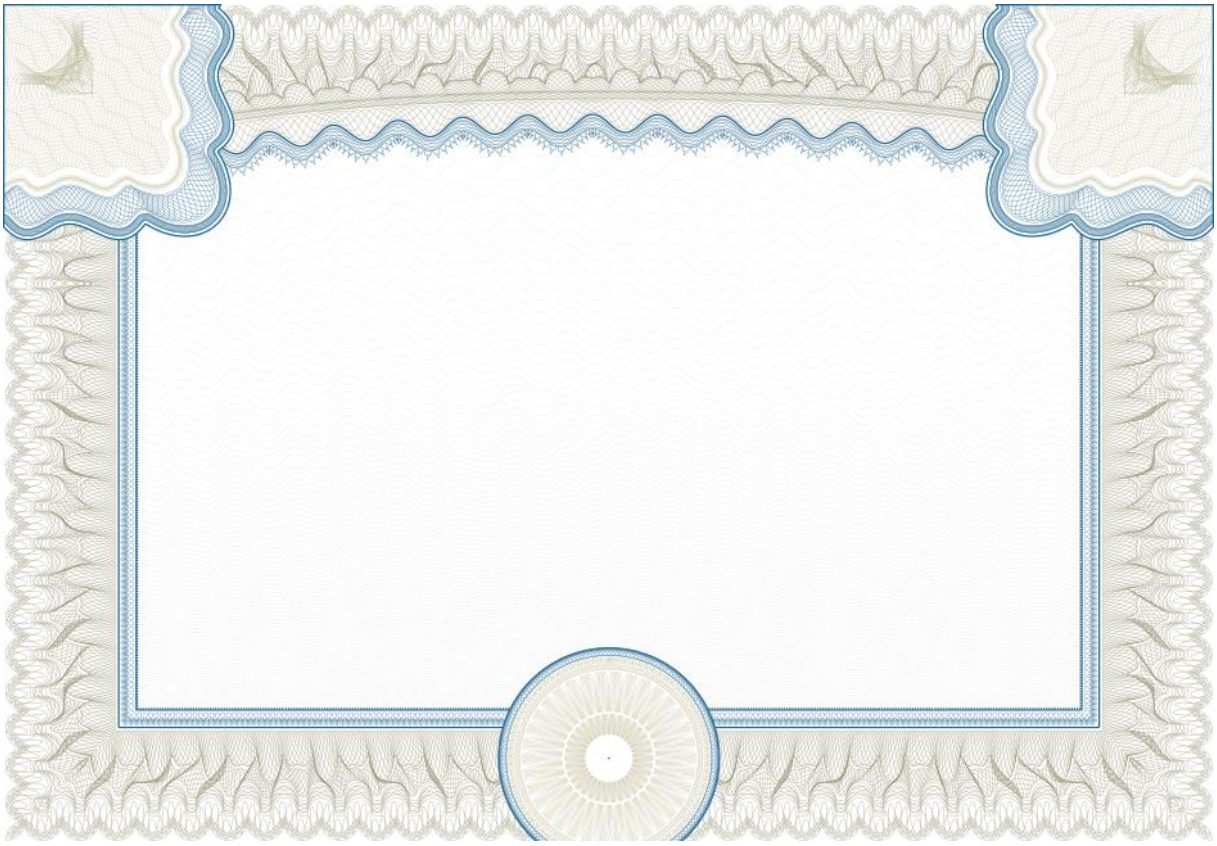

Figure 1: Diplome vierge

Quelles informations stocker en clair dans le diplôme ?

Lors de la conception du système de diplômes, il est crucial de déterminer quelles informations doivent être accessibles sans aucune forme de protection. Les éléments tels que le numéro de diplôme servent à garantir l'unicité de chaque document, permettant ainsi une traçabilité efficace. De même, le nom et prénom de l'étudiant, en conjonction avec sa date de naissance, fournissent une identification précise et fiable. La date d'obtention du diplôme est essentielle pour établir le contexte temporel de la réalisation de l'accomplissement académique, tandis que l'intitulé du diplôme et celui de la formation définissent clairement les qualifications obtenues. Enfin, mentionner le nom de l'établissement confère une légitimité institutionnelle au document, renforçant ainsi sa crédibilité. La moyenne de l'étudiant et sa mention sont des indicateurs cruciaux de ses performances académiques et sont donc inclus pour une évaluation transparente.

Figure 2: Diplome avec informations en clair

Quelles informations stocker chiffrées / stéganographiées dans le diplôme ?

Certaines données sensibles nécessitent une protection supplémentaire pour éviter toute altération ou accès non autorisé. Le numéro de diplôme, bien qu'il soit également stocké en clair, est chiffré pour empêcher toute manipulation malveillante pouvant compromettre l'authenticité du document. De même, une signature contenant les informations stéganographiées est ajoutée pour garantir son intégrité et son origine légitime, ainsi que de garantir la non-altération des données fournies. Enfin, les notes et coefficients de l'étudiant, en tant qu'informations confidentielles, sont stéganographiés pour empêcher toute modification ou accès non autorisé, assurant ainsi la confidentialité des résultats académiques.

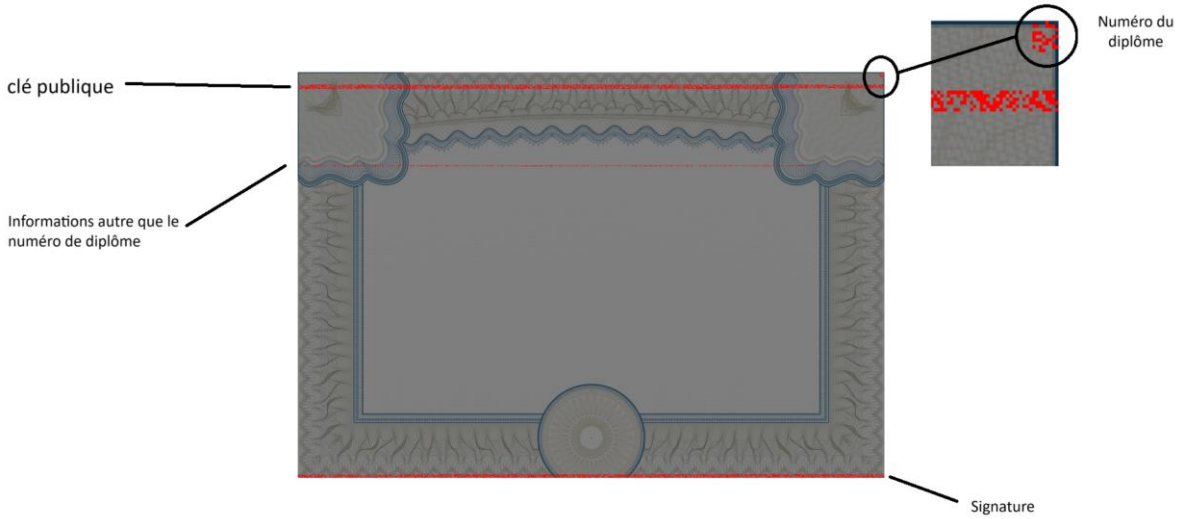

Figure 3: Highlight des informations stéganographiées dans le diplôme

Figure 4: Diplôme généré à la fin

Figure 5: Différence entre le diplôme de base et le diplôme final

Qui peut vérifier le diplôme ?

La vérification du diplôme est un processus ouvert à tous les tiers intéressés par l'authenticité d'un document académique. Cependant, la génération des diplômes est réservée exclusivement à l'établissement d'enseignement délivrant le document. Cette distinction est cruciale pour garantir l'intégrité du processus de certification et empêcher toute falsification. Pour assurer la validité de la signature du diplôme, celle-ci est vérifiable en utilisant la clé publique de l'établissement, une information sécurisée stockée à la fois dans le diplôme et dans un système de stockage sécurisé appartenant à l'établissement. La vérification peut se faire dans le script via la commande *checkDiplome*

Comment générer le diplôme ?

Le processus de génération du diplôme est une étape critique dans la sécurisation de l'authenticité et de l'intégrité du document. Tout d'abord, les informations claires sont intégrées dans le diplôme pour établir une base de données précise et accessible. Ensuite, les informations supplémentaires telles que le numéro de diplôme, les notes, les coefficients, le nom et prénom de l'étudiant sont stéganographiées pour une sécurité renforcée, empêchant ainsi toute altération ou falsification. Par la suite, la signature du diplôme avec comme base les données ci-dessus est appliquée à l'aide de la clé privée de l'établissement, garantissant ainsi son authenticité et son origine légitime. Enfin, la signature est intégrée au diplôme en utilisant une technique stéganographique spécifique, assurant ainsi la cohérence et l'intégrité du document.

Comment vérifier le diplôme ?

La vérification du diplôme est une procédure rigoureuse visant à garantir son authenticité et son intégrité. Tout d'abord, les informations stéganographiées sont extraites du diplôme pour être analysées. Ensuite, la signature du diplôme est retirée en annulant les modifications

stéganographiées, permettant ainsi une évaluation précise de son authenticité. La validité de la signature est ensuite vérifiée en utilisant la clé publique de l'établissement, confirmant ainsi son origine légitime. Par la suite, les informations présentes dans la signature sont comparées aux informations stéganographiées pour confirmer leur correspondance, garantissant ainsi l'authenticité et l'intégrité du diplôme. En cas de correspondance, les informations cachées sont fournies au vérificateur pour une validation complète du diplôme, confirmant ainsi son authenticité et son intégrité. Ce processus rigoureux assure la validité et la sécurité des diplômes délivrés par l'établissement, renforçant ainsi la confiance dans le système éducatif.

```
Traceback (most recent call last):
  File "C:\Users\romro\Documents\M2\info002\tp2\main.py", line 320, in <module>
    main(cmd, sys.argv[2:])
  File "C:\Users\romro\Documents\M2\info002\tp2\main.py", line 291, in main
    print(checkDiplome(args[0]))
  File "C:\Users\romro\Documents\M2\info002\tp2\main.py", line 244, in checkDiplome
    raise Exception("Invalid signature")
Exception: Invalid signature
```

Figure 6: Erreur lors de la vérification de la signature

```
C:\Users\romro\Documents\M2\info002\tp2\env\Scripts\python.exe C:\Users\romro\Documents\M2\info002\tp2\main.py
('Diploma is valid hiddenwise', '84za5zs21d', 'HYVERNAT', 'Pierre', [('INFO907', 20.0, 2), ('INFO908', 19.0, 13), ('INFO909', 18.0, 8)], 18.74)

Process finished with exit code 0
```

Figure 7: Les informations correspondent à ce qui est marqué dans le diplôme, il est valide

```
C:\Users\romro\Documents\M2\info002\tp2\env\Scripts\python.exe C:\Users\romro\Documents\M2\info002\tp2\main.py
('Diploma is valid hiddenwise', 'abcdefghij', 'HYVERNAT', 'Pierre', [('INFO907', 20.0, 1000), ('INFO908', 19.0, 13), ('INFO909', 20.0, 8)], 19.99)

Process finished with exit code 0
```

Figure 8: Les informations stéganographiées correspondent à celles présentes dans la signature, mais diffèrent de ce qui est marqué dans le diplôme, il est invalide

Failles de sécurité potentielles et solutions envisagées

Malgré les efforts déployés pour concevoir un système de génération et de vérification de diplômes robuste, quelques failles de sécurité potentielles pourraient subsister. Parmi celles-ci, on peut citer :

1. Altération de la signature : Même si la signature du diplôme est faite via une clé privée, une faille dans la gestion des clés ou une compromission de la clé privée pourrait permettre à un attaquant de générer de fausses signatures.

2. Modification des données claires accolées aux données stéganographiées : Il est possible d'apposer les informations stéganographiées sur un nouveau diplôme dont on aurait altéré les informations en clair.

Pour atténuer ou supprimer ces risques, plusieurs solutions sont envisagées :

1. Gestion sécurisée des clés : Une gestion rigoureuse des clés privées et publiques, avec des mécanismes de rotation et de protection adéquats, peut réduire le risque de compromission des clés.

2. Vérifications par le vérificateur des informations entrées : bien que les informations stéganographiées soient valides, il faut un utilisateur pour vérifier que les informations stockées correspondent aux informations en clair. Une idée d'amélioration serait de rajouter de la reconnaissance d'image afin de comparer les données stéganographiées aux données en clair automatiquement, et fournir une vérification manuelle en cas de litige ou de doute.