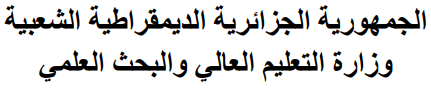
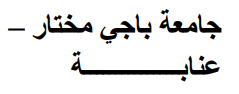


****

**UniversitéBadjiMokhtar - Annaba BadjiMokhtar**

**Faculté : Technologie**

**Département : Informatique**

**Domaine : Mathématique-Informatique**

**Filière : Informatique**

**Spécialité : Ingénierie des logicielles complexes**

**Le Chiffrement avec Hill-ADN**

**Présenté par : Hamza Loudjaine**

**Nasser Chaima**

**Hamana Racha Supervisé par : Mme Souisi**

**Année Universitaire: 2023/2024**

**Table des matière**

**1.Introduction…………………………………………………………………………………4**

**2.Chiffrement avec l’algorithme Hill-ADN …………………………………………………4**

**3.Déchiffrement avec l’algorithme Hill-ADN ……………………………………………….4**

**4.Conception UML…………………………………………………………………………….5**

**5.Points forts …………………………………………………………………………………..7**

**6.Conclusion …………………………………………………………………………………...7**

**Table de Figure**

1.Figure 1 : Diagramme de Cas d’utilisation ………………………………………………….5

2.Figure 2 : Diagramme de Class ……………………………………………………………..6

3.Figure 3 : Diagramme de Séquence ………………………………………………………..6

**1.Introduction**

La cryptographie de Hill, développée par Lester S. Hill dans les années 1920, repose sur l'utilisation de matrices pour chiffrer et déchiffrer des messages. Cette méthode classique a évolué avec le temps, donnant naissance à des approches hybrides, notamment la cryptographie basée sur l'ADN. L'ADN, en tant que porteur efficace de l'information génétique, offre des perspectives prometteuses pour renforcer la sécurité des données échangées. Dans cette optique, nous explorons l'hybridation de la cryptographie de Hill avec la cryptographie basée sur l'ADN, en intégrant des concepts biologiques tels que les structures d'ADN et d'acides aminés pour améliorer le processus de chiffrement.

**2.Chiffrement avec l’algorithme Hill-ADN :**

1. **Première étape : Conversion en binaire et transformation en ADN**
   * Conversion du texte clair en binaire 8-bit.
   * Transformation du binaire en ADN selon la règle (A(00), C(01), G(10), T(11)).
   * Application de la règle ADN pour obtenir la forme ADN [DP].
2. **Deuxième étape : Passage à la table d’Acides aminés**
   * Utilisation d'une table d'Acides aminés pour traduire la séquence ADN en un texte avec un alphabet spécifique.
   * Consultation du tableau des acides aminés pour obtenir le résultat intermédiaire.
3. **Troisième étape : Chiffrement avec l'algorithme de Hill**
   * Le texte obtenu à l'étape précédente, avec son nouvel alphabet, peut être chiffré avec l'algorithme de Hill.
   * Utilisation d'une clé de chiffrement spécifique pour appliquer des transformations linéaires aux blocs de lettres.

**3.Déchiffrement avec l’algorithme Hill-ADN :**

1. **Première étape : Déchiffrement avec l'algorithme de Hill**
   * Utilisation de la clé de déchiffrement correspondante pour inverser les transformations linéaires appliquées lors du chiffrement.
2. **Deuxième étape : Conversion de la séquence déchiffrée**
   * Le texte déchiffré sera dans le nouvel alphabet.
   * Utilisation de la table d'Acides aminés inverse pour obtenir la séquence ADN correspondante.
3. **Troisième étape : Conversion de l'ADN en texte binaire**
   * Inversion de la transformation ADN vers le binaire selon la règle inverse (A(00), C(01), G(10), T(11)).
4. **Quatrième étape : Conversion du binaire en texte clair**
   * Transformation du binaire 8-bit en texte clair pour retrouver le message initial.

L'ensemble de ces étapes assure le processus complet de chiffrement et de déchiffrement utilisant l'algorithme Hill-ADN.

**4.Conception UML**

Dans la suite de cette présentation, nous plongerons de manière approfondie dans la conception de différentes figures cruciales qui joueront un rôle central dans l'explication des concepts que nous abordons. Ces représentations graphiques incluront des diagrammes de cas d'utilisation, de classes et de séquence, soigneusement élaborés pour mettre en lumière des aspects spécifiques et assurer la clarté et la cohérence de nos explications. Ces schémas ont été créés dans le but de rendre accessible et visuellement informatif le contenu technique que nous allons explorer.

1. **Diagramme de Cas d’utilisation**

|  |
| --- |
|  |
| **Figure 1 : Diagramme de CU** |

1. **Diagramme de Class**

|  |
| --- |
|  |
| **Figure 2 : Diagramme de class** |



1. **Diagramme de Séquence**

|  |
| --- |
| [2] |
| **Figure 3 : Diagramme de Séquence (chiffrement et déchiffrement)** |

**5.Points forts**

1. **Complexité biologique renforcée** : L'intégration de l'ADN et des acides aminés rend le chiffrement plus robuste, complexifiant la compréhension et la tentative de violation par des attaquants.
2. **Densité de stockage élevée** : L'ADN permet d'encapsuler de vastes quantités de données dans un espace restreint, potentiellement utilisé pour des clés de chiffrement plus longues et complexes.
3. **Contournement d'attaques classiques** : Les méthodes traditionnelles de piratage peuvent être contournées grâce à la complexité introduite par l'utilisation de l'ADN, rendant notamment les attaques par force brute plus ardues.
4. **Combinaison de techniques** : L'hybridation entre la cryptographie classique et les éléments biologiques renforce la sécurité globale du système en tirant profit des avantages des deux approches.
5. **Résilience face aux attaques informatiques** : L'ADN n'étant pas habituellement ciblé par les attaques informatiques, la méthode Hill-ADN pourrait être moins vulnérable à certaines attaques traditionnelles.
6. **Stockage sur support biologique** : L'utilisation de l'ADN comme support de stockage offre une durabilité et une résilience pour stocker des données de manière biologique.
7. **Stimulus pour l'innovation interdisciplinaire** : En unissant cryptographie et biologie, le Hill-ADN peut stimuler l'innovation dans la sécurité de l'information en favorisant des approches interdisciplinaires.

**6.Conclusion**

En conclusion, ces figures ne sont pas simplement des éléments visuels, mais des outils stratégiques qui renforcent la compréhension des concepts présentés. Leur exploration approfondie guidera notre parcours à travers la complexité des sujets à venir. Nous invitons donc à suivre attentivement ces schémas, car ils joueront un rôle essentiel dans l'assimilation et la maîtrise des concepts abordés dans cette présentation.