REPUBLIQUE DEMOCRATIQUE DU CONGO
ENSEIGNEMENT SUPERIEUR ET UNIVERSITAIRE
UNIVERSITE DE L'ASSOMPTION AU CONGO
« U.A.C »

Site : www.uaconline.edu.cd
E-mail : contact@uaconline.edu.cd

B.P. : 104 BUTEMBO/Nord-Kivu

FACULTÉ DE SCIENCES ECONOMIQUES ET DE GESTION
DÉPARTEMENT INGENERIE ET MANAGEMENT DES SYSTEMES D'INFORMATIONS

« TP D'ÉLÉMENTS DE CRYPTOGRAPHIE ET DE CRYPTANALYSE»

Par **: KABUNGA KITENGERA Christelle**

KASOKI LUHALA Christelle

Tuteur :KAMBALE SYATSUKWA Alfred

Chef des travaux

ANNEE ACADEMIQUE : 2024-2025

Q1) Implémenter un outil qui permet de déchiffrer un message chiffré avec l'algorithme de César sans connaître la clé de chiffrement en appliquant l'analyse fréquentielle. Afficher les 5 résultats de déchiffrement les plus probables.

```
Python 3.12.3 (tags/v3.12.3:f6650f9, Apr  9 2024, 14:05:25) [MSC v.1938 64 bit
AMD64)] on win32
Type "help", "copyright", "credits" or "license()" for more information.

= RESTART: C:/Users/NF/Downloads/tpcryptoCesar.py
Entrez le message chiffré à déchiffrer : ibaltiv
Essai 1 (Décalage 4): exwhper
Essai 2 (Décalage 23): ledowly
Essai 3 (Décalage 22): mfepxmz
Essai 4 (Décalage 7): butembo
Essai 5 (Décalage 15): tmlwetg
```

Les codes sont dans le fichier : tpcryptoCesar.py

Q2) Implémenter un outil de chiffrement et déchiffrement en AES avec un langage de votre choix. Avec différents modes selon le choix de l'utilisateur si possible: ECB, CBC, CTR, OFB, CFB, …

```
Entrez le texte à chiffrer : Bonjour, ceci est un test en AES !
Choisissez le mode (ECB, CBC, CTR, OFB, CFB) : CBC
```

```
Texte chiffré : 5J3XcFqUpjQ8rx6pJuejGUbM7Q+oZHbUym2pjw92xEJ7cL8Wf5Wm7w==
Texte déchiffré : Bonjour, ceci est un test en AES !
```

Les codes : cfr fichier chiffrementAES.py

Q3) À l'aide du tableau d'entiers ci-dessous, convertissez les nombres en caractères ASCII correspondants pour obtenir le message clair. Utilisez un langage de programmation de votre choix [78, 79, 85, 83, 32, 89, 32, 65, 76, 76, 79, 78, 83, 32, 68, 69, 77, 65, 73, 78, 32, 77, 65, 84, 73, 78]

```
========== RESTART: C:/Users/NF/Downloads/tpExamCrypto/codeASCII.py ==========
Message clair : NOUS Y ALLONS DEMAIN MATIN
```

Les codes : cfr fichier codeASCII.py

Q4) Ce message est codé en Base64, trouvez le message clair: UkVTVEVSIENIQUNIySwgSUxTIE9OVCBEyUNPVVZFUlQgVk9UUkUgSVA=

```
Message clair : RESTER CHACUN, ILT ONT DÉCOUVERT VOTRE IP
```

Les codes : cfr fichier base64.py

Q5) Essayé de trouver le message à partir de cette représentation binaire: 01000011 01000101 00100000 01010001 01010101 01001001 00100000 01000101 01010011 01010100 00100000 01010110 01010010 01000001 01001001 00101100 00100000 01010010 01001001 01000101 01001110 00100000 01001110 00100111 01000101 01010011 01010100 00100000 01000111 01000001 01010010 01000001 01001110 01010100 01001001

```
============ RESTART: C:/Users/NF/Downloads/tpExamCrypto/binaire.py ============
Message clair : CE QUI EST VRAI, RIEN N'EST GARANTI
```

Q6) Faites une recherche sur les différentes méthodes cryptanalytiques des différents algorithmes de chiffrement classiques (Affine, Vigenère, Hill et Rail Fence).

0. Introduction

La cryptographie classique repose sur des méthodes de chiffrement qui ont évolué au fil des siècles pour protéger les communications. Parmi ces méthodes, les algorithmes de chiffrement classiques comme **Affine**, **Vigenère**, **Hill** et **Rail Fence** ont joué un rôle clé dans la sécurisation des messages. Cependant, ces algorithmes, bien qu'ingénieux pour leur époque, présentent des vulnérabilités qui ont été exploitées par des techniques de cryptanalyse. Cette analyse explore les méthodes cryptanalytiques utilisées pour déchiffrer ces systèmes, en mettant en lumière leurs forces et leurs faiblesses (Amara Korba, 2022).

Parallèlement, la cryptographie moderne a évolué pour répondre aux besoins croissants de sécurité dans un monde de plus en plus numérique. Contrairement à la cryptographie classique, qui reposait principalement sur des techniques de substitution et de transposition, les méthodes modernes manipulent des bits plutôt que des caractères alphabétiques. Cette transition a permis de renforcer la sécurité des systèmes cryptographiques, en s'appuyant sur des algorithmes complexes et des clés de grande taille. Parmi les algorithmes les plus connus, on trouve le **DES (Data Encryption Standard)** et son successeur, l'**AES (Advanced Encryption Standard)**, qui sont largement utilisés pour protéger les données sensibles dans les transactions en ligne et les communications sécurisées (Rezkallah, 2007).

Les problèmes **NP-Complets**, tels que le problème du sac à dos ou la factorisation d'entiers, jouent également un rôle crucial dans la conception des systèmes cryptographiques modernes. Ces problèmes, réputés difficiles à résoudre, fournissent une base solide pour la sécurité des algorithmes à clé publique comme **RSA**. En effet, la difficulté à factoriser de grands nombres composés garantit que les messages chiffrés avec RSA restent sécurisés, même face à des attaques sophistiquées. L'utilisation de problèmes NP-Complets en cryptographie offre ainsi une garantie théorique de sécurité, bien que des avancées futures en calcul quantique pourraient remettre en cause cette approche (Rezkallah, 2007).

Enfin, les travaux de **Thomas Izard (2011)** sur l'optimisation des opérateurs arithmétiques parallèles pour la cryptographie asymétrique montrent l'importance de l'efficacité des calculs modulaires et des opérations sur les courbes elliptiques. Ces protocoles cryptographiques nécessitent des calculs intensifs sur des opérandes de grande taille (plusieurs centaines à milliers de bits), rendant cruciale l'efficacité de l'arithmétique multiprécision et modulaire. Izard propose des algorithmes parallèles exploitant les architectures multicœurs et les processeurs graphiques (GPU) via des interfaces comme OpenMP et CUDA. Ces travaux permettent des gains significatifs en temps de calcul, avec des applications directes pour des protocoles comme RSA et ECC (Izard, 2011).

METHODES CRYPTANALYTIQUES DES ALGORITHMES CLASSIQUES

1. Chiffrement Affine :

Le chiffrement Affine utilise une fonction mathématique simple pour transformer chaque lettre du message. Bien que cette méthode soit facile à mettre en œuvre, elle est vulnérable à l'analyse des fréquences. En effet, les lettres d'un texte chiffré avec Affine conservent les mêmes fréquences que dans le texte original, ce qui permet à un cryptanalyste de déduire la clé en analysant les répétitions de lettres. Par exemple, en français, les lettres les plus fréquentes (comme E, A, S) peuvent être identifiées et utilisées pour reconstituer la clé (Rezkallah, 2007).

2. Chiffrement de Vigenère :

Le chiffrement de Vigenère est plus complexe que celui d'Affine, car il utilise une clé répétée pour décaler les lettres du message. Cependant, il reste vulnérable à des attaques comme le test de Kasiski. Cette méthode consiste à repérer des séquences de lettres répétées dans le texte chiffré, ce qui permet de deviner la longueur de la clé. Une fois la longueur de la clé connue, l'analyse des fréquences peut être appliquée pour déchiffrer le message (Rezkallah, 2007).

3. Chiffrement de Hill :

Le chiffrement de Hill utilise une matrice pour transformer des groupes de lettres. Bien que cette méthode soit plus robuste que les précédentes, elle peut être cassée si l'attaquant dispose d'un texte clair connu. En connaissant une partie du message original et son équivalent chiffré, il est possible de reconstituer la matrice de chiffrement et de déchiffrer le message entier (Rezkallah, 2007).

4. Chiffrement Rail Fence :

Le Rail Fence est une méthode de transposition qui réorganise les lettres du message en les écrivant en zigzag sur plusieurs lignes. Bien que simple, cette méthode est vulnérable à des attaques basées sur la reconnaissance de motifs. Un cryptanalyste peut essayer différentes configurations de lignes pour retrouver le texte original, surtout si le message est court ou si des indices sur sa structure sont disponibles (Rezkallah, 2007).

Conclusion

Les algorithmes de chiffrement classiques comme Affine, Vigenère, Hill et Rail Fence ont marqué l'histoire de la cryptographie en offrant des méthodes simples pour protéger les communications. Cependant, leur vulnérabilité aux techniques de cryptanalyse, telles que l'analyse des fréquences, le test de Kasiski ou la reconnaissance de motifs, a conduit à leur remplacement par des systèmes plus robustes. Ces méthodes classiques restent néanmoins essentielles pour comprendre les bases de la cryptographie et les défis liés à la sécurisation des données (Rezkallah, 2007).

Références :

1. Rezkallah, L. (2007). De la cryptographie classique à la cryptographie moderne : Théorie et application (Mémoire de Magister). Université des Sciences et de la Technologie Houari Boumediène, Faculté des Mathématiques.
2. Amara Korba, K. (2022). La Sécurité des Réseaux de Capteurs sans fil Multimédia par des Systèmes Chaotiques (Thèse de doctorat). Université du 08 mai 45, Guelma, Algérie. https://theses.hal.science/tel-03787403
3. Izard, T. (2011). Opérateurs Arithmétiques Parallèles pour la Cryptographie Asymétrique (Thèse de doctorat, Université Montpellier II - Sciences et Techniques du Languedoc). HAL. https://theses.hal.science/tel-00685654