Butembo, le 13-12-2024

TP D'ÉLÉMENTS DE CRYPTOGRAPHIE ET DE CRYPTANALYSE

1. 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.

2. 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, …

3. 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]

4. Ce message est codé en Base64, trouvez le message clair:

   UkVTVEVSIENIQUNIySwgSUxTIE9OVCBEyUNPVVZFUlQgVk9UUkUgSVA=

5. 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

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

Bon travail

Ir Alfred Syatsukwa