Kakaev
Ibrahim

Compte rendu
TP Crypto

String → Tableau binaire :

Le code fourni convertit une chaîne de caractères en un tableau d'entiers représentant les bits de chaque caractère. Il gère également les caractères spéciaux et les majuscules en utilisant des manipulations bit à bit. L'opération de décalage de bits (`>>`) est utilisée pour extraire les bits d'un caractère, tandis que l'opération logique `&` extrait le bit le plus à droite. Ainsi, chaque caractère est représenté par une séquence spécifique de bits dans le tableau d'entiers final. Cette méthode facilite le stockage et la manipulation des caractères en tant que séquences de bits, simplifiant ainsi les opérations ultérieures sur les données.

Test effectuer :

testBitsString() : Ce test vérifie si la conversion d'une chaîne de caractères en bits, suivie de sa reconversion en chaîne de caractères, donne la même chaîne de caractères que celle d'origine. Cela permet de s'assurer que les méthodes de conversion entre chaînes de caractères et bits fonctionnent correctement.

testDecoupage() : Ce test vérifie si la fonction "decoupage" sépare correctement un tableau d'entiers en blocs de la taille spécifiée. Il compare ensuite le résultat obtenu avec un tableau 2D d'entiers attendu pour vérifier l'exactitude du découpage.

testRecollage_bloc() : Ce test vérifie si la fonction "recollage_bloc" peut reconstituer correctement un tableau unique à partir d'un tableau 2D de blocs, en s'assurant que le tableau reconstitué correspond exactement au tableau d'entiers attendu.

testPermutation() : Ce test vérifie si la fonction "permutation" effectue une permutation sur un tableau d'entiers selon les règles spécifiées. Il compare le résultat de la permutation avec un tableau d'entiers attendu pour s'assurer de la précision de la fonction de permutation.

testPermutationInv() : Ce test vérifie si la fonction "invPermutation" effectue une permutation inverse sur un tableau d'entiers comme prévu. Il compare le résultat de la permutation inverse avec un tableau d'entiers attendu pour garantir la précision de la fonction d'invPermutation.

testDecalageAGauche() : Ce test vérifie si la fonction "decalle_gauche" décale correctement un tableau d'entiers vers la gauche d'un nombre spécifié de crans. Il compare le résultat du décalage avec un tableau d'entiers attendu pour garantir que le décalage à gauche se déroule comme prévu.

testXor() : Ce test vérifie si la fonction "xor" effectue correctement l'opération XOR (OU exclusif) entre deux tableaux d'entiers. Il compare le résultat de l'opération XOR avec un tableau d'entiers attendu pour s'assurer que l'opération XOR se déroule comme prévu.

testFonctionS() : Ce test vérifie si la fonction "fonction_S" applique correctement la substitution de bits selon les règles spécifiées pour l'algorithme DES. Il compare le résultat de la substitution avec un tableau d'entiers attendu pour garantir l'exactitude de la fonction de substitution.

testCrypteDecrypte() : Ce test chiffre un message à l'aide de l'algorithme DES, puis tente de le déchiffrer pour vérifier si le résultat final correspond au message d'origine. Cela permet de garantir que les fonctions de chiffrement et de déchiffrement de l'algorithme DES fonctionnent correctement et sont réversibles.

Mon DES peut faire les 16 Rondes

Modification :

- J’ai ajouter dans la fonction fonction_F le tableau P pour effectuer les permutation demander

Triple DES :

Ma classe TripleDES utilise ces 2 méthodes pour le 3DES :

Chiffrement :

La méthode chiffrement prend une chaîne de caractères message en entrée.
Elle effectue d'abord un tour de chiffrement en appelant la méthode crypto de l'objet des de la classe DES avec le message donné en argument.
Ensuite, elle chiffre à nouveau le résultat en utilisant les méthodes bitsToString et crypto de l'objet des.
Enfin, elle chiffre une troisième fois le résultat en utilisant de nouveau les méthodes bitsToString et crypto de l'objet des.
La méthode retourne le texte chiffré sous forme d'un tableau d'entiers.

Déchiffrement :

La méthode dechiffrement prend un tableau d'entiers texteChiffre en entrée.
Elle commence par décrypter une première fois le texte chiffré en appelant la méthode decrypto de l'objet des avec le texte chiffré en argument.
Ensuite, elle déchiffre une deuxième fois le résultat en utilisant les méthodes stringToBits et decrypto de l'objet des.
Enfin, elle déchiffre une troisième fois le résultat en utilisant de nouveau les méthodes stringToBits et decrypto de l'objet des.
La méthode retourne le texte déchiffré sous forme d'une chaîne de caractères.

Interface graphique :

→ On lance la Classe Main

On démarre sur une interface d'accueil ou on a le choix entre le cryptage DES et 3DES et donc on choisit l'une ou l'autre en appuyant sur l'un des boutons puis on arrive sur une autre interface diviser en 2 avec 2 zone de texte et 2 boutons.

-Crypter : On rentre le message a coder dans la zone de texte gauche et on appuie sur le bouton crypter puis apparaîtra a droite le résultat du cryptage.

-Décrypter : On rentre les donnes crypter dans la zone de texte droite et on appuie sur le boutons décrypter puis apparaîtra le message decrypter.