**UNIVERSITE DE KINSHASA**

**FACULTE DE SCIENCE**

**DEPARTEMENT DE MATH-INFO**

B.P. 190 KINSHASA XI



TRAVAIL PRATIQUE

COURS : TRANSMISSION DES DONNEES ET LA SECURITE INFORMATIQUE

|  |  |
| --- | --- |
| **Rédiger par l’étudiant :** |  |
|  | MUTOMBO MUTOMBO EMMANUEL |
|  | L2 GENIE |
|  | COURS DISPENSE PAR : |
|  | PROF. Kasengedia Motumbe Pierre  Assité par : Junior Kaningini  Jacque Mayombo  Emmanuel Mbamba |

Année-académique : 2021-2022

**ALGORITHME DE GENERATION DES CLES**

public static int[] generateKey(int[] perm, int shiftOrder) {

int[] key = {0, 1, 2, 3, 4, 5, 6, 7};

for (int i = 0; i < shiftOrder; i++) {

int temp = key[0];

System.arraycopy(key, 1, key, 0, key.length - 1);

key[key.length - 1] = temp;

}

int[] newKey = new int[8];

for (int i = 0; i < perm.length; i++) {

newKey[i] = indexOf(key, perm[i]);

}

return newKey;

}

private static int indexOf(int[] array, int value) {

for (int i = 0; i < array.length; i++) {

if (array[i] == value) {

return i;

}

}

return -1;

}

**ALGORITHME DE CHIFFREMENT DES CLES**

public static String encrypt(String plaintext, int[] key) {

StringBuilder ciphertext = new StringBuilder();

for (int i = 0; i < plaintext.length(); i += 8) {

char[] block = plaintext.substring(i, i + 8).toCharArray();

char[] newBlock = new char[8];

for (int j = 0; j < key.length; j++) {

newBlock[j] = block[key[j]];

}

ciphertext.append(newBlock);

}

return ciphertext.toString();

}

**ALGORITHME DE DECHIFFREMENT DES CLES**

public static String decrypt(String ciphertext, int[] key) {

StringBuilder plaintext = new StringBuilder();

for (int i = 0; i < ciphertext.length(); i += 8) {

char[] block = ciphertext.substring(i, i + 8).toCharArray();

char[] newBlock = new char[8];

for (int j = 0; j < key.length; j++) {

newBlock[key[j]] = block[j];

}

plaintext.append(newBlock);

}

return plaintext.toString();

}