TP2

Exercice 1

1-

2- On effectue un XOR bit à bit entre les messages possibles et les messages chiffré :

M1ꚛC = 0110 0110 1111 0011 0010 0100 0011 1000 🡪 14 différences

M2ꚛC = 0110 1101 0010 1110 1101 0110 1010 1100 🡪 22 différences

M3ꚛC = 1110 0111 1000 0111 1110 0011 1001 1100 🡪 9 différences

D’après la question 1, on attend une différence de 8 bits (32/4 = 8 = ¼). À la vue des différences, (14, 22 et 9 respectivement), le message clair le plus probable est la message 3.

Exercice 2

1-

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| X1(t) | X2(t) | X3(t) | Z(t) | X1(t) = Z(t) | X3(t) = Z(t) |
| 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 0 | 1 | 1 | 0 | 1 |
| 0 | 1 | 0 | 0 | 1 | 1 |
| 1 | 0 | 0 | 0 | 0 | 0 |
| 0 | 1 | 1 | 0 | 1 | 1 |
| 1 | 0 | 1 | 1 | 1 | 0 |
| 1 | 1 | 0 | 1 | 1 | 1 |
| 1 | 1 | 1 | 1 | 1 | 1 |
|  |  |  |  | 6/8 = 3/4 | 6/8 = 3/4 |

D’après la table ci-dessus, Le résultat de Z(t) est égal à X1(t) 3 fois sur 4 tout comme X3(t) par rapport à Z(t)