# Solution

## **Cryptage (k, a = 4 ; b = 5)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cryptosystème** | **Letters** | **Demarches** | **Résultats** |
| **Additif**  **(x + k) % 26** | U (20) | (20 + 4 ) % 26 = **24** | Y (24) |
| S (18) | (18 + 4 ) % 26 = **22** | W (22) |
| R (17) | (17 + 4 ) % 26 = **21** | V (21) |
| **Multiplicatif**  **(k x) % 26** | U (20) | (4 **×** 20) % 26 = **80 % 26 = 2** | C (2) |
| S (18) | (4 **×** 18) % 26 = **72 % 26 = 20** | U (20) |
| R (17) | (4 **×** 17) % 26 = **68 % 26 = 16** | Q (16) |
| **Affine**  **(a x + b) % 26** | U (20) | (4 **×** 20 + 5) % 26 = **85 % 26 = 7** | H (7) |
| S (18) | (4 **×** 18 + 5) % 26 = **77 % 26 = 25** | Z (25) |
| R (17) | (4 **×** 17 + 5 ) % 26 = **73 % 26 = 21** | V (21) |

|  |  |
| --- | --- |
| **Cryptosystème** | **Message Crypté** |
| **Additif** | Ywiv mrmxmexih viqsxi ibigyxmsr exxegow jsv ibeqtpi lswxmpi aif wmxi Xvsner lsvwi iqemp erh ws sr |
| **Multiplicatif** | Cuqq gagygayqm qqweyq qoqicygea ayyaiou ueq qoawisq ceuygsq kqe ugyq Yqekaa cequq qwags aam ue ea |
| **Affine** | Hzvv lfldlfdvr vvbjdv vtvnhdljf fddfntz zjv vtfbnxv hjzdlxv pvj zldv Dvjpff hjvzv vbflx ffr zj jf |

## **Décryptage (méthode force brute)**

***Note :*** *Seule le mot en rouge est utilisé pour la démarche avec cryptosytéme additif,* ***message*** *=**Vjg kpigpwkva qh vjg etkokpcnu ku* ***nkokvnguu***

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Cryptosystème** | **Demarches** | | | | | | | | | | **Detail**  **(letter N)** |
| **Additif**  **(x - k) % 26** | **Clé (k)** | **N (13)** | **K (10)** | **O (14)** | **K (10)** | **V (21)** | **N (13)** | **G (6)** | **U (20)** | **U (20)** |
| **1** | M (12) | J (9) | N (13) | J (9) | U (20) | M (12) | F (5) | T (19) | T(19) | **13 – 1 % 26 = 12 (M)** |
| **2** | **L (10)** | **I (8)** | **M (12)** | **I (8)** | **T (19)** | **L (11)** | **E (4)** | **S (18)** | **S(18)** | **13 – 2 % 26 = 10 (L)** |
| **Cryptosystème** | **Message Original** | | | | | | | | | | |
| **Additif , k = 2** | The ingenuity of the criminals is limitless | | | | | | | | | | |
| **Multiplicatif (Echéc)** |  | | | | | | | | | | |
| **Affine, k = 1** | The ingenuity of the criminals is limitless | | | | | | | | | | |

Affine (avec k = 1) aussi peut décrypter le message car (x - 2) % 26 = (1) (x - 2) % 26, tq : a = 1, b = 2