**Licence L2 STS Mention SPI Parcours Informatique**
**Unité 174EN007**
**Sécurité Informatique**

# Correction TD4

Ce TD porte sur différents aspects cryptologiques.

## Exercice n°1 : le chiffre de Hill

| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Coder le message LE TD EST FINI sachant que m=2, a=3, b=5, c=1 et d=2.
$y_1 = 3x_1 + 5x_2$
$y_2 = x_1 + 2x_2$

| Etape 1 | LE | TD | ES | TF | IN | IA |
|---|---|---|---|---|---|---|
| Etape 2 | 11 ; 4 | 19 ; 3 | 4 ; 18 | 19 ; 5 | 8 ; 13 | 8 ; 0 |
| Etape 3 | 53 ; 19 | 72 ; 25 | 102 ; 40 | 82 ; 29 | 89 ; 34 | 24 ; 8 |
| Etape 4 (modulo 26) | 1 ; 16 | 20 ; 25 | 24 ; 14 | 4 ; 3 | 11 ; 8 | 24 ; 8 |
| Etape 5 | BT | UZ | YO | ED | LI | YI |

Décoder le message EUOCEMYOWITZFT avec les mêmes paramètres.

$y_1 = 2x_1 - 5x_2$
$y_2 = -x_1 + 3x_2$

| Etape 1 | EU | OC | EM | YO | WI | TZ | FT |
|---|---|---|---|---|---|---|---|
| Etape2 | 4 ; 20 | 14 ; 2 | 21 ; 14 | 24 ; 14 | 22 ; 8 | 19 ; 25 | 5 ; 19 |
| Etape 3 | -92 ; 56 | 18 ; -8 | -52 ; 32 | -22 ; 18 | 4 ; 2 | -87 ; 56 | -85 ; 52 |
| Etape 4 (modulo 26) | 12 ; 4 | 18 ; 18 | 0 ; 6 | 4 ; 18 | 4 ; 2 | 17 ; 4 | 19 ; 0 |
| Etape 5 | M E | S S | A G | E S | E C | R E | T A |

## Exercice n°2 : le chiffre de Vernam et le chiffre du Che

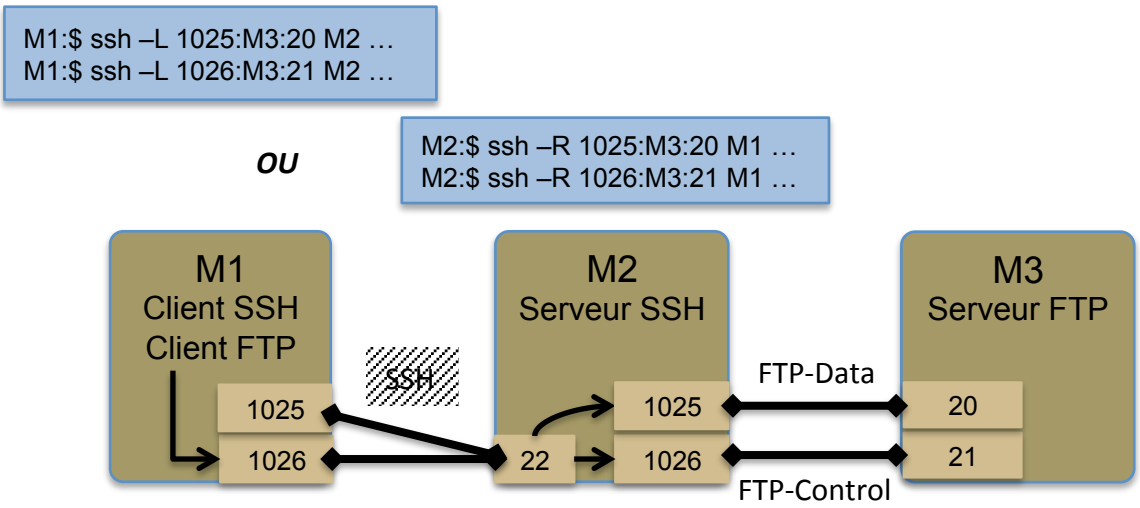
Décoder le message 9790327590062385783956 sachant que la clé commence par 1582327192042355486317.

$m + k = c$
$m = c - k$

| A | 06 | E | 08 | I | 39 | M | 70 | Q | 71 | U | 52 | Y | 01 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| B | 38 | F | 30 | J | 31 | N | 76 | R | 58 | V | 50 | Z | 59 |
| C | 32 | G | 36 | K | 78 | O | 09 | S | 02 | W | 56 | | |
| D | 04 | H | 34 | L | 72 | P | 79 | T | 00 | X | 54 | | |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| c | 97 90 3 | | | 27 59 0 | | | | 06 23 8 | | | | 57 83 9 | | | 56 | |
| k | 15 82 3 | | | 27 19 2 | | | | 04 23 5 | | | | 54 86 3 | | | 17 | |
| m = c - k | 82 08 0 | | | 00 40 8 | | | | 02 00 3 | | | | 03 97 6 | | | 39 | |
| m décodé | 82 = L | 08 = E | | 00 = T | 04 = D | | 08 = E | 02 = S | | 00 = T | | 30 = F | 39 = I | | 76 = N | 39 = I |

**Exercice n°3 : redirection de port avec SSH**




**Exercice n°4 : étude des messages TLS v1.2**