Cryptographie

UE OP6.33

Nour Boulahcen

April 29, 2020

Institut Villebon Georges Charpak

Table of contents

Introduction

Demarche

Le but de cette UE était de décoder 8 messages et chacun de ces messages nous donne une information sur comment a été chiffré le message suivant. Cela nous a amené a devoir implenter 4 chiffres:

- Scytale
- Caesar
- Vigenere
- Enigma

Chiffre par transposition - `Scytale`

Implementation

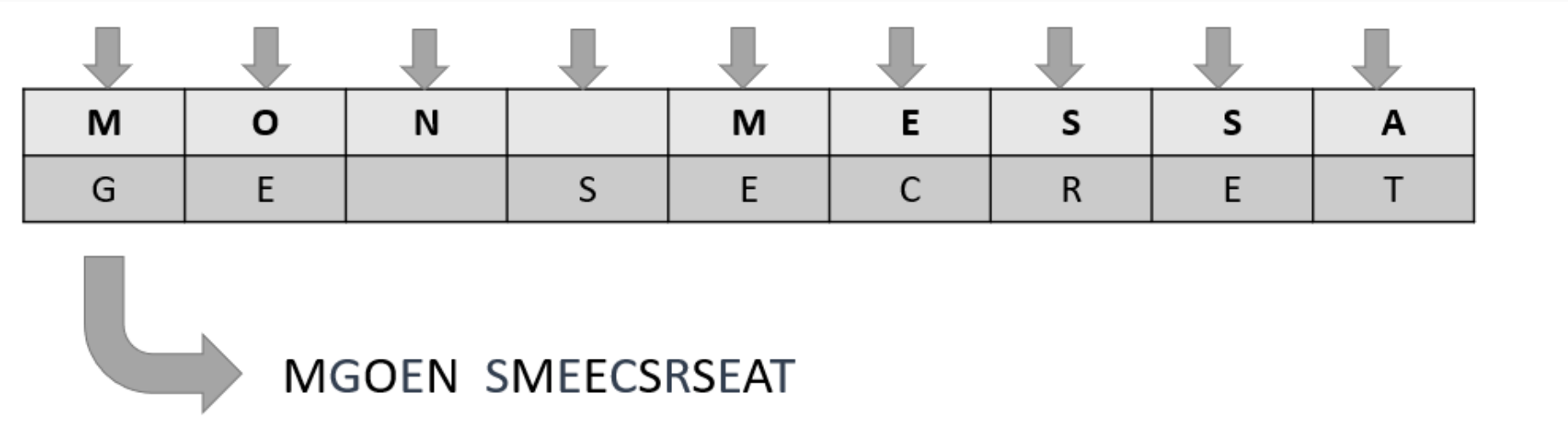


Figure 1: Chiffrement par Scytale

Implementation

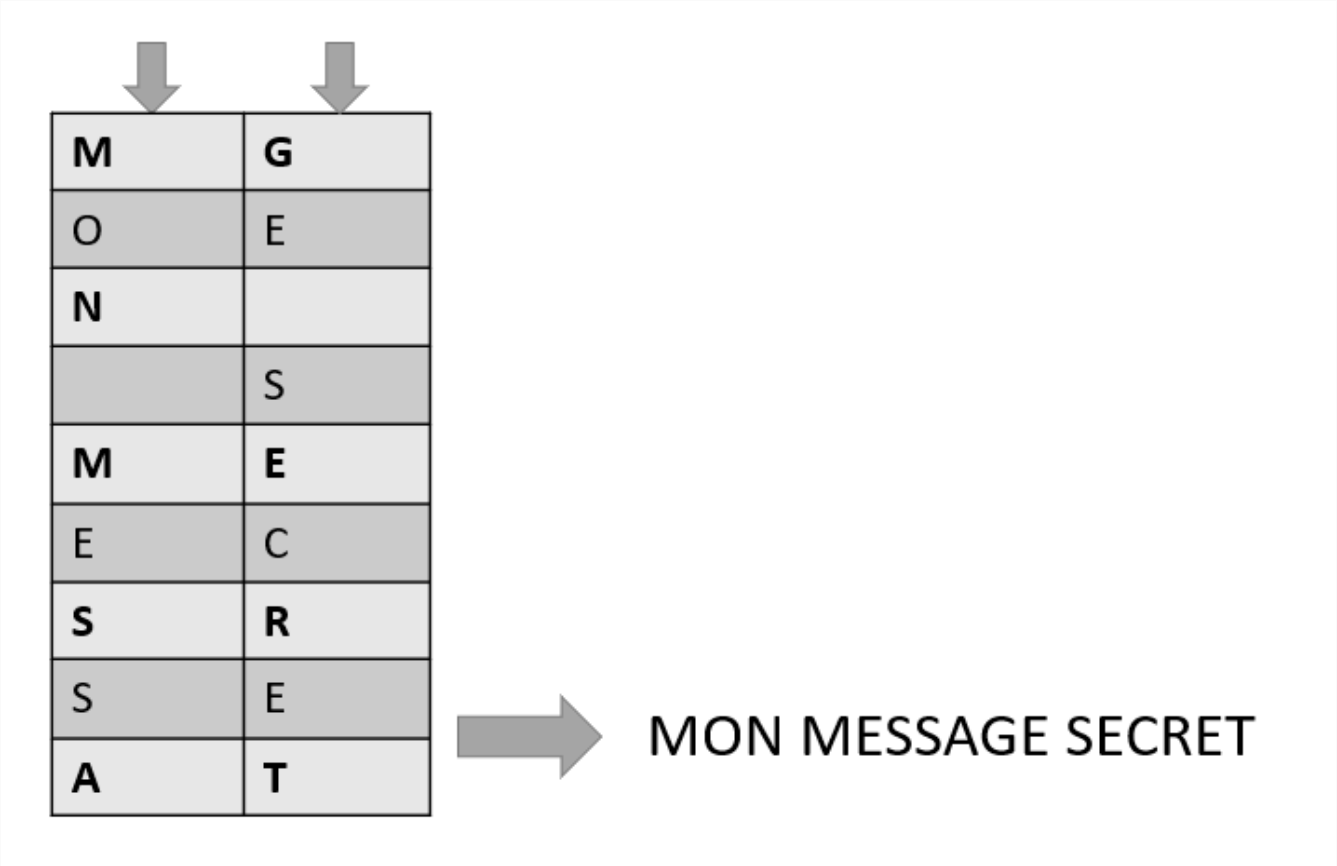


Figure 2: Dechiffrement par Scytale

Attaque Brutforce

- Autant de tentative que de caractère
- Filtre par **mot clé** (Joël)
- S'arrête quand le mot clé est trouvé
- **Complexité en** $O(n^2(n+1)/2+n)$

Chiffre par substitution - César/Vigenere

Implementation

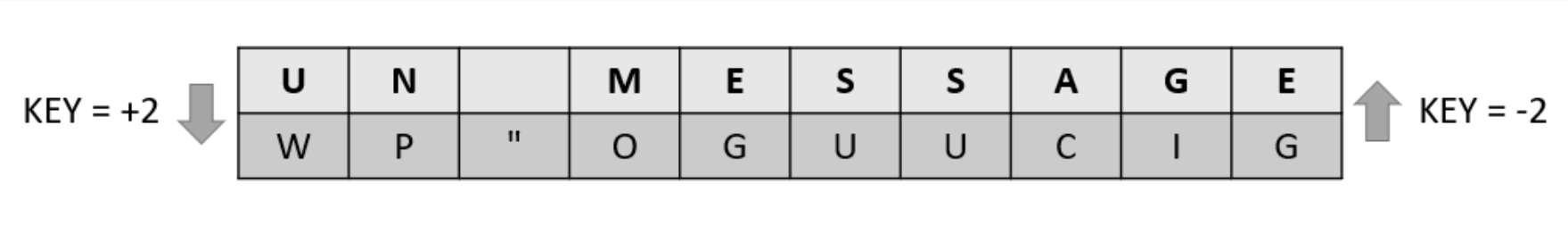


Figure 3: Chiffre de Caesar

Implementation

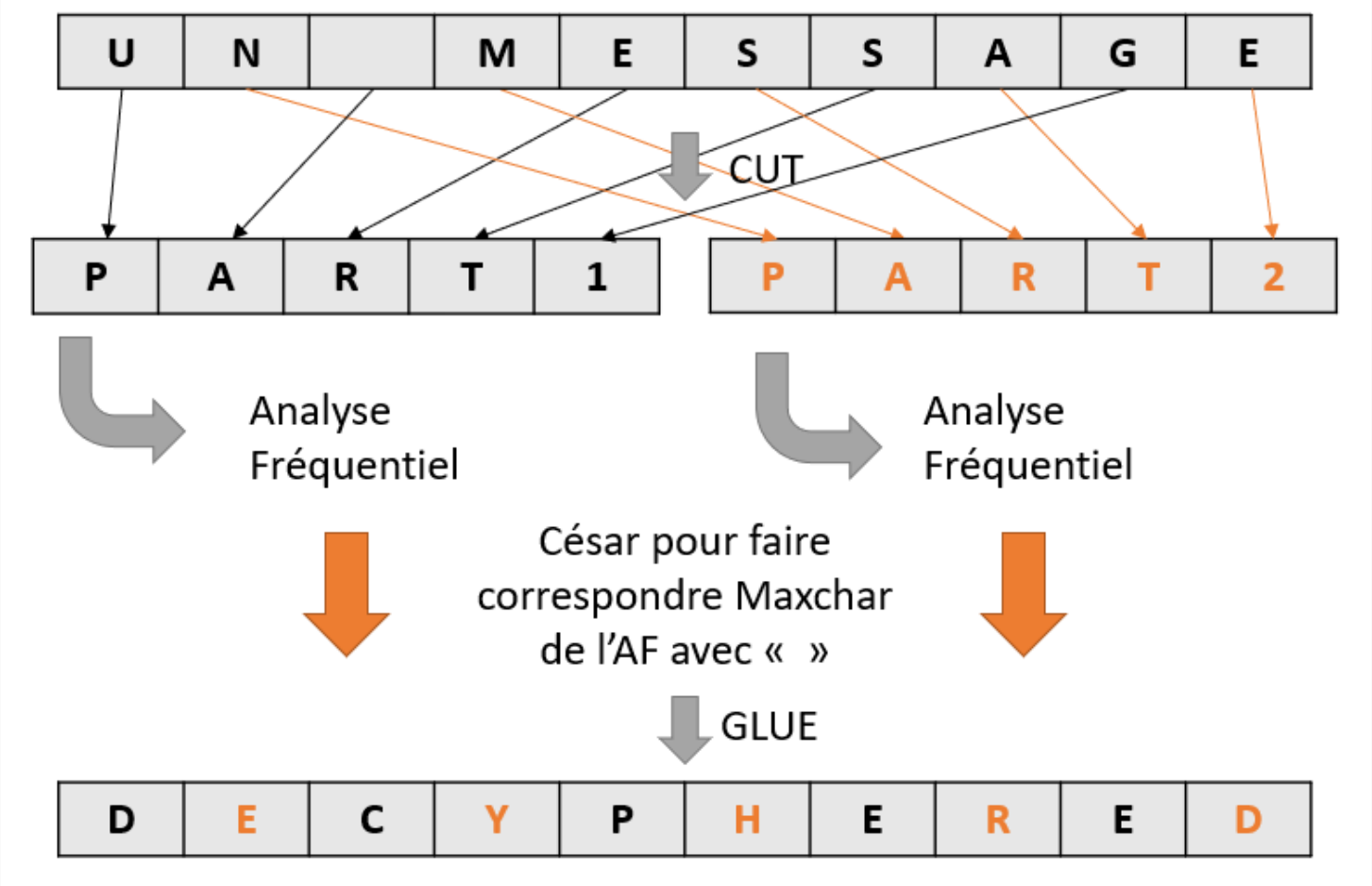


Figure 4: Chiffre de Vigenere

Attaque Brutforce

- Autant de tentative que de caractère (attaque sur la découpe)
- On essaie de deviner le décalage du césar par **AF**
- Pour que l'AF soit efficace, le texte doit être **assez long**
- Filtre par **mot clé** (Joël)
- S'arrête quand le mot clé est trouvé
- **Complexité en** $O(n^4 + n^3 + n^2 + n)$

Enigma

Implementation

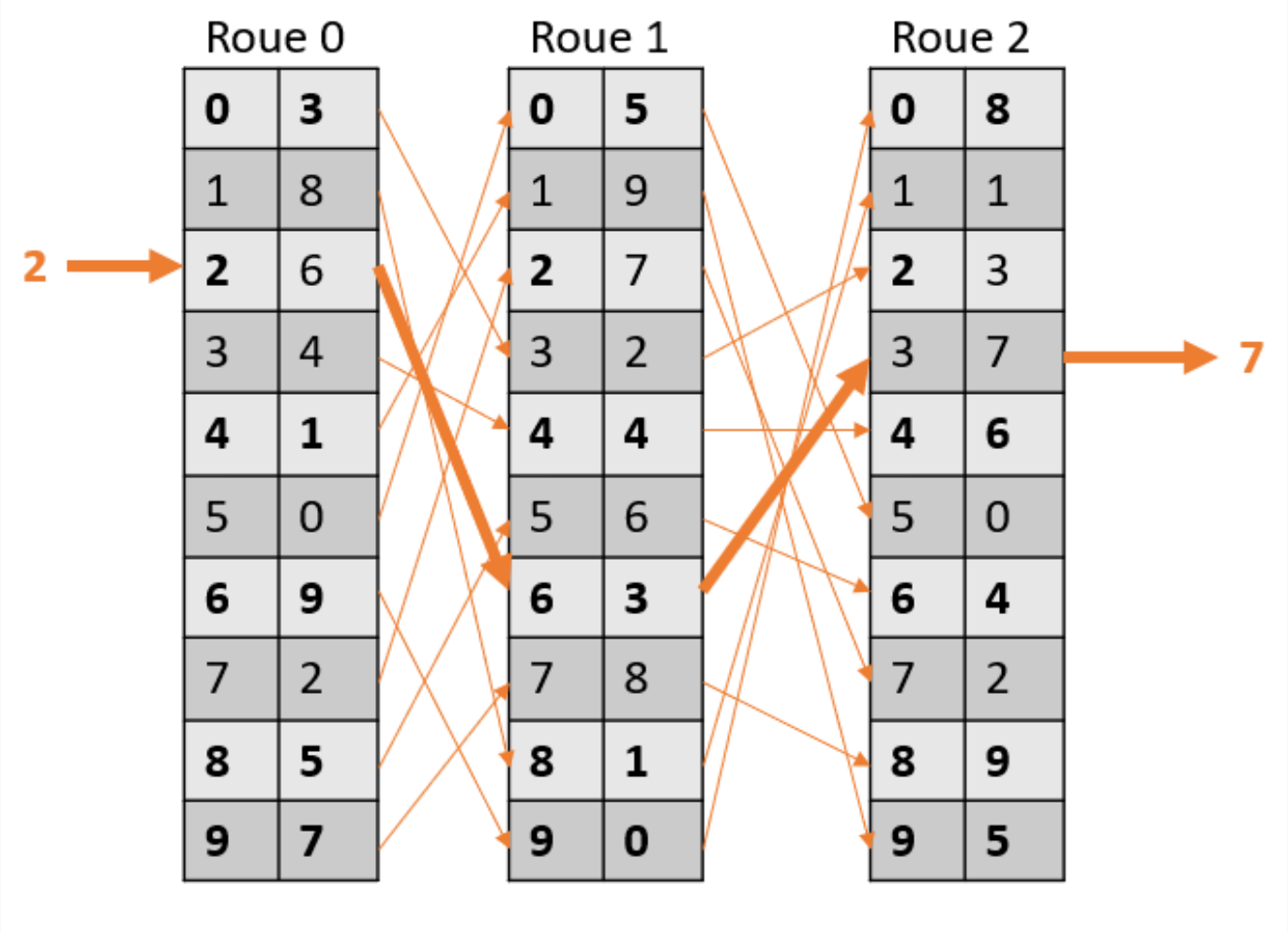


Figure 5: Encodage d'un caractère par Enigma

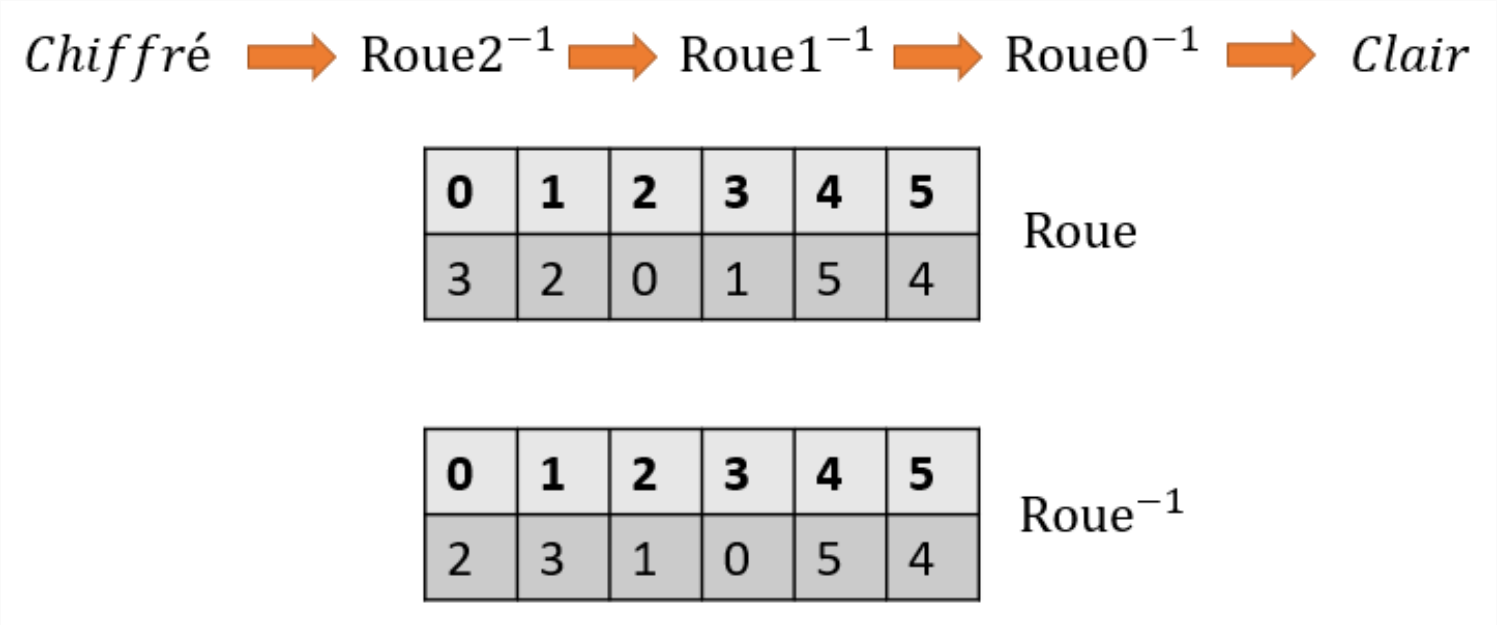
Implementation

- Pour chaque caractère, la roue 0 tourne d'un cran
- Pour chaque tour complet de la roue 0, la roue 1 tourne d'un cran
- Pour chaque tour complet de la roue 1, la roue 2 tourne d'un cran

Implementation

Faire tourner les roues et encoder le caractère est équivalent a faire tourner le carctère l'encoder puis de le faire tourner dans l'autre sens : $ABA^{-}1 \equiv B$

Implementation



0	1	2	3	4	5
3	2	0	1	5	4

0	1	2	3	4	5
2	3	1	0	5	4

Figure 6: Décodage d'un texte par Enigma

Attaque Brutforce

- On a 3 parmis 8 combinaisons de roues et 3 parmis 256 position initale
- Supposition: le premier mot du message est ”Félicitation”
- On brutforce donc uniquement les 13 premiers char pour trouver la clé
- Une fois la clé trouvé, on peut décrypter le message entier
- Pour plus de rapidité pour le brutforce, on pourait l'implementer en C

Questions?