

2024  
2025

# Travaux Pratiques n°2

## Les primitives cryptographiques

CNAM – RSX112 – SECURITE DES RESEAUX

STEPHANE LARCHER



# Travaux pratiques

## Les primitives cryptographiques

## Table des matières

Le texte.....	3
ATELIER : ANALYSE DE FRÉQUENCES ET DÉCHIFFREMENT D'UN TEXTE SIMPLE .....	3
1. Objectif de l'atelier .....	3
2. Matériel nécessaire.....	3
3. Déroulement.....	3
Étape 1 : Découverte du texte chiffré.....	3
Étape 2 : Calcul des fréquences .....	3
Étape 3 : Comparaison avec les fréquences usuelles .....	4
Étape 4 : Établissement d'hypothèses de substitution .....	4
Étape 5 : Validation et affinage.....	4
Étape 6 : Approfondissement .....	4

## Le texte

FHWWH PHWKRGH GDQDOBVH GH IUHTXHQFHV PRQWUH LD YXOQHUDELOLWH GXQ  
FKLIIUHPHQW D VXEVLWXWLRQ VLPSON ERQQH FKDQFH SRXU OH GHFKLIIUHU

## ATELIER : ANALYSE DE FRÉQUENCES ET DÉCHIFFREMENT D'UN TEXTE SIMPLE

### 1. Objectif de l'atelier

- i. Apprendre à **casser** un chiffrement simple (substitution monoalphabétique ou Chiffre de César) en utilisant l'**analyse de fréquences**.
- ii. Comprendre pourquoi les **chiffrements classiques** basés sur une simple substitution sont **facilement vulnérables** aux attaques statistiques.

### 2. Matériel nécessaire

- i. Un **texte chiffré** (fourni en annexe ou sur feuille séparée).
- ii. Une **table** ou un **tableur** (papier, Excel, etc.) pour compter les occurrences des lettres.
- iii. (Optionnel) Un **logiciel** ou un **script** pour automatiser le comptage des fréquences.
- iv. Un **tableau des fréquences moyennes** des lettres dans la langue concernée (français ou anglais).

### 3. Déroulement

#### Étape 1 : Découverte du texte chiffré

- i. **Lisez le texte chiffré** distribué. Il s'agit d'un court paragraphe ou d'une liste de mots dans laquelle les lettres ont été substituées.
- ii. **Notez vos premières impressions** :
  - a. Repérez si certaines lettres semblent revenir très souvent,
  - b. Repérez s'il y a des répétitions de groupes de lettres ou des motifs particuliers.

#### Étape 2 : Calcul des fréquences

- i. **Listez toutes les lettres de l'alphabet** (A à Z) dans un tableau ou un tableur.
- ii. **Parcourez le texte chiffré** et comptez le nombre de fois où chaque lettre apparaît.
  - a. Ignorez la ponctuation, les espaces et les chiffres.

- iii. **Calculez la fréquence relative** en divisant le nombre d'occurrences de chaque lettre par le nombre total de lettres dans le texte.
  - a. Exprimez cette fréquence sous forme de pourcentage ou de fraction décimale.

### Étape 3 : Comparaison avec les fréquences usuelles

- i. **Classez les lettres** de la plus fréquente à la moins fréquente dans votre texte.
- ii. **Comparez** votre classement avec le **tableau de fréquences habituelles** dans la langue visée.
  - a. En français, la lettre la plus fréquente est souvent "E", suivie de "S", "A", "R"...
  - b. En anglais, "E", "T", "A", "O", etc.

### Étape 4 : Établissement d'hypothèses de substitution

- i. **Faites correspondre** la lettre la plus fréquente dans le texte chiffré à la lettre la plus fréquente de la langue (par exemple, "X" → "E").
- ii. **Testez cette hypothèse** :
  - a. Appliquez la substitution sur quelques mots du texte.
  - b. Regardez si cela forme des séquences de lettres cohérentes (ex. « LE », « DE », « ET » en français).
- iii. **Poursuivez avec les autres lettres**, en vous aidant de votre tableau de fréquences.

### Étape 5 : Validation et affinage

- i. **Substituez progressivement** les lettres selon vos hypothèses, puis **tentez de lire** les bouts de mots obtenus.
- ii. **Identifiez les incohérences** :
  - a. Par exemple, si vous vous apercevez que « SAA » ne correspond à rien de lisible, vérifiez si votre hypothèse sur la correspondance est erronée.
- iii. **Ajustez** en conséquence :
  - a. Inversez les correspondances conflictuelles,
  - b. Recherchez des digrammes courants ("LE", "DE", "EN", "RE" en français) et vérifiez s'ils apparaissent dans votre texte.

### Étape 6 : Approfondissement

- i. **Digrammes et trigrammes** :
  - a. Repérez les paires de lettres fréquemment associées (ex. "QU", "ER", "ES" en français).
  - b. Comparez-les avec les paires que vous voyez dans le texte chiffré.

- ii. **Position des lettres :**
  - a. Observez les lettres en début et fin de mot, très utiles pour repérer des petits mots comme “LE”, “LA”, “UN” en français.
- iii. **Terminez la substitution** et vous devriez obtenir un **texte clair** lisible.