# Le chiffrement ADFGVX

**Principe :** Ce système de codage est basé sur le principe du carré de Polybe mais on utilise un carré 6x6
Il y a donc …... cases : …. lettres de l'alphabet + ….....

**Exemple :** On choisit le carré c08xf4mk3az9nw1ojd5siyhuplvb6req7t2g .
On complète alors un carré 6 x 6 de gauche à droite en sachant que les lignes et les colonnes sont repérées non pas par les chiffres de 1 à 6 mais par les lettres ADFGVX

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Le codage :** On veut coder le message suivant : OBJECTIF PARIS 15 H

Sur le principe du carré de POLYBE, on obtient :

**La force de cette méthode : LA PERMUTATION**

**1ère étape :** On choisit alors un mot de passe (ici on prendra NOTREDAME) et on recopie le message codé en dessous (une lettre par case) et de gauche à droite :

| N | O | T | R | E | D | A | M | E |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Il reste ici des cases vides. On les complète alors par des lettres quelconques parmi ADFGVX .

**2ème étape:** On numérote alors le mot de passe de 1 à 9 (ici) et on le réécrit dans l'ordre alphabétique dans un autre tableau.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

On dit alors que la permutation est :

**3ème étape:**
On transmet alors le message codé en lisant ce dernier tableau de haut en bas puis de gauche à droite :

Ce système fut inventé par le colonel allemand FRITZ NEBEL durant l'année 1918. Au début, ce chiffre n'utilisait pas le V et on parlait du chiffre ADFGX. Ces lettres ont été choisies car leurs correspondances en morse étaient très distinctes ce qui évitait les erreurs de transmission. Pour des raisons de Secret Défense, les exploits du Capitaine Painvin ne furent révélés qu'en 1960 et son inventeur, le colonel NEBEL, ne l'apprit qu'en 1967. Il était persuadé que son système était resté inviolé .

**A vous de Jouer**

Coder le message suivant à l'aide de ce système de chiffrement et le mot de passe POLYBE :

**Message :** Renfort attendu à 15 h 43

Codage avec la grille précédente :

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

**Permutation :**

**Codage final :**

Reprendre alors le radiogramme de la victoire et chercher à le décoder :
Un indice de taille : le mot clé est composé de 9 lettres
(on pourra pour cela découper les bandes ci-dessous)

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |