# Séance 1 - Travaux Dirigés
# Chiffrements historiques

Yann Rotella

2026

## Partie 1 - seul.e - 1h

**Exercice 1.** *La Scytale.*
On s'échauffe.

(1) Combien y'a t'il de transpositions possibles pour un message de longueur $n$ ?
Le message suivant a été chiffré à l'aide d'une scytale.

```
lunlaessatsadueatebamtmeuiaalfsqieonuncrooaht
```

(2) Quel est le diamètre de la scytale ? Quel est le message clair ?

(3) *À la maison :* À partir de quelle valeur de $n$ avons-nous un nombre de clefs possibles (pour un chiffrement par transposition) supérieur au nombre de clefs d'Enigma ? On pourra s'aider d'un ordinateur si besoin.

**Exercice 2.** *Substitution et transposition seules.*
Question de cours :

(1) Quelle est la faiblesse d'un chiffrement par substitution ? Combien y'a t'il de clefs possibles dans un chiffrement par substitution mono-alphabétique général ?

On souhaite renforcer la sécurité d'un chiffrement par substitution mono-alphabétique en effectuant d'abord un chiffrement par transposition particulier (avec une scytale) puis un chiffrement par substitution.

(2) Donner la description mathématique de ces deux transformations. On veillera à donner les espaces de départ et les espaces d'arrivée. On supposera pour se simplifier que les messages à chiffrer sont des multiples du nombre de caractères mis dans un tour de la scytale, noté $\ell$.

(3) Que pensez-vous de la sécurité de ce cryptosystème ? Justifier. Et si on compose plusieurs transpositions et substitutions ?

(4) *À la maison :* Si on limite le diamètre de la scytale à $d$ et que l'unité d'écriture d'un caractère est de 1 et que l'alphabet considéré est de $n$ caractères, combien (approximativement) de clefs y'a t'il dans ce cryptosystème ?

**Exercice 3.** *Sécurité des mots de passe.*
Pour chacun des schémas de mots de passe suivants, indiquer le nombre de combinaisons qu'une attaque par force brute (effectuée par quelqu'un qui connaîtrait le schéma) devra tester pour être certaine de trouver le mot de passe.

(1) On impose exactement 8 caractères minuscules, mais les lettres ne doivent pas se répéter.

(2) On impose des lettres minuscules ou majuscules pour les 5 premiers caractères et des chiffres pour les 3 derniers caractères.

(3) On impose exactement 7 caractères minuscules ou majuscules et exactement 2 caractères spéciaux (15 possibilités)

(4) *À la maison :* On impose de 6 à 10 caractères composés uniquement de minuscules, majuscules ou chiffres.

(5) *À la maison :* On impose exactement 8 caractères minuscules, majuscules ou caractères spéciaux, où le nombre de caractères spéciaux est au plus 2.

# Partie 2 - Enigma - en groupe - 2h

Dans cet exercice nous allons considérer le modèle M3 de la machine ENIGMA, utilisée par l'armée allemande. Cette machine est composée des éléments suivants :

— Un **clavier** comportant les lettres `A` à `Z`.

— Un **tableau de connexions** permettant de relier deux lettres du clavier entre elles.

— Trois **rotors** choisis parmi un ensemble de cinq rotors possibles (notés I, II, III, IV et V) et placés dans un ordre particulier. Sur une face d'un rotor sont disposés en cercle des contacts électriques à aiguilles. Sur l'autre face, sont disposés le même nombre de contacts plats. Les contacts plats et à aiguilles représentent l'alphabet (lettres de 'A' à 'Z'). Une fois les rotors assemblés, les contacts à aiguilles d'un rotor se positionnent en face des contacts plats du rotor voisin, formant ainsi la connexion électrique. À l'intérieur du rotor, un ensemble de 26 câbles électriques assurent les connexions entre les contacts à aiguilles et les contacts plats suivant un chemin concret pour chaque rotor. Chaque rotor représente une permutation de 26 lettres.

  Chaque fois qu'on chiffre une lettre, les rotors avancent. Plus précisément, à chaque nouvelle touche pressée, seulement le premier rotor (le rotor le plus à gauche) avance d'un cran. Le rotor du milieu avance d'une position seulement quand le premier rotor se trouve à une position particulière, appelée *position d'entraînement*. Le troisième rotor avance quand le deuxième rotor se trouve à sa propre position d'entraînement.

— Un **réflecteur**, placé à droite des trois rotors est une dernière permutation qui permet de revenir en arrière. On permute une dernière fois les lettres deux par deux, et on les fait retraverser les rotors et le tableau de connexion.

— Un **tableau lumineux**.

Les permutations décrivant les cinq rotors ainsi que celle correspondant au réflecteur sont présentées dans le tableau suivant :

| | 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Rotor** | 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 | 26 |
| **I** | 5 | 11 | 13 | 6 | 12 | 7 | 4 | 17 | 22 | 26 | 14 | 20 | 15 | 23 | 25 | 8 | 24 | 21 | 19 | 16 | 1 | 9 | 2 | 18 | 3 | 10 |
| **II** | 1 | 10 | 4 | 11 | 19 | 9 | 18 | 21 | 24 | 2 | 12 | 8 | 23 | 20 | 13 | 3 | 17 | 7 | 26 | 14 | 16 | 25 | 6 | 22 | 15 | 5 |
| **III** | 2 | 4 | 6 | 8 | 10 | 12 | 3 | 16 | 18 | 20 | 24 | 22 | 26 | 14 | 25 | 5 | 9 | 23 | 7 | 1 | 11 | 13 | 21 | 19 | 17 | 15 |
| **IV** | 5 | 19 | 15 | 22 | 16 | 26 | 10 | 1 | 25 | 17 | 21 | 9 | 18 | 8 | 24 | 12 | 14 | 6 | 20 | 7 | 11 | 4 | 3 | 13 | 23 | 2 |
| **V** | 22 | 26 | 2 | 18 | 7 | 9 | 20 | 25 | 21 | 16 | 19 | 4 | 14 | 8 | 12 | 24 | 1 | 23 | 13 | 10 | 17 | 15 | 6 | 5 | 3 | 11 |
| **Réfl.** | 25 | 18 | 21 | 8 | 17 | 19 | 12 | 4 | 16 | 24 | 14 | 7 | 15 | 11 | 13 | 9 | 5 | 2 | 6 | 26 | 3 | 23 | 22 | 10 | 1 | 20 |

Les positions d'entraînement des rotors I, II, III, IV et V sont respectivement `Q`, `E`, `V`, `J` et `Z`.

**Exercice 4.** *Schéma du cryptosystème.*
Dessiner votre représentation complète de la machine Enigma du modèle M3, en supposant que la sélection des rotors a été réalisée.

**Exercice 5.** *Taille de la clé.*
La configuration de l'ENIGMA est donnée par :

— Le choix (ordonné) de 3 rotors parmi 5.
— La position de départ de chaque rotor.
— Les positions d'entraînement des rotors du gauche et du milieu.
— La configuration du tableau de connexions, qui peut lier jusqu'à 13 paires de lettres.

(1) Donner le nombre de possibilités pour choisir 3 parmi les 5 rotors et les ordonner.

(2) Donner le nombre de positions de départ possibles pour les trois rotors.

(3) Donner le nombre de positions possibles pour l'entraînement des rotors du gauche et du milieu.

(4) Donner le nombre de configurations possibles du tableau de connexions quand une paire de lettres est permutée. Faire pareil pour $2, 3, \ldots, 13$ paires de lettres. En déduire le nombre total de configurations possibles du tableau de connexions.

(5) Donner la formule mathématique décrivant le nombre total de configurations possibles pour cette ENIGMA.

**Exercice 6.** *Chiffrement et déchiffrement.*
Considérons une configuration simple de l'ENIGMA : Les rotors III, II et I (de gauche à droite) sont utilisés et on suppose pour l'instant qu'aucune paire de lettres n'est connectée par le tableau de connexions.

(1) En quelle lettre `A` sera-t-elle chiffrée avec une telle configuration ?

(2) En commençant avec la même configuration, en quelle lettre sera chiffrée la lettre `N` ? Pour cette question, il n'y a *a priori* pas besoin de faire de calculs.

(3) Montrer que la propriété trouvée à la question d'avant est valable pour toute lettre. On veillera à formaliser correctement la propriété avant de la montrer.

On lie maintenant certaines lettres par le tableau de connexion.

(4) En quelles lettres seront chiffrées `A` et `R` si on suppose que les lettres `A-C` et `R-X` sont liées ?

(5) En quelles lettres seront chiffrées `A` et `N` si on suppose qu'elles sont liées par le tableau de connexions ?

(6) Une lettre peut-elle être chiffrée en elle-même ? Pourquoi ?

**Exercice 7.** *Cryptanalyse d'ENIGMA.*
Chaque jour, tous les opérateurs ENIGMA commençaient par taper chaque message en utilisant les mêmes réglages, comme spécifiés dans le carnet des codes pour ce jour particulier. Cependant, afin d'assurer une meilleure sécurité, ils choisissaient différents messages-clés (positions de rotors) pour chaque nouveau message.

Le mode d'utilisation pour chiffrer un message donné était le suivant :

— Régler la machine selon les réglages du jour spécifiés dans le carnet des codes.
— Taper le message-clé choisi deux fois (e.x. `BITBIT` ).
— Régler les rotors à la position indiquée par le message-clé (e.x. `BIT` ici).
— Taper le message actuel.

Un opérateur qui recevait le message allait effectuer les actions suivantes afin de le déchiffrer :

— Régler la machine selon les réglages du jour spécifiés dans le carnet des codes.
— Recevoir et déchiffrer les six premiers caractères, vérifiant que la répétition a eu lieu, et extraire le message-clé.
— Régler les rotors à la position indiquée par le message-clé.
— Déchiffrer le reste du message chiffré.

Toutefois, un tel chemin comporte un point extrêmement faible que nous allons exploiter dans cet exercice.

Le tableau suivant présente un nombre de message-clés chiffrés, interceptés pendant le même jour (c.-à.-d. chiffrés avec les réglages initiaux d'Enigma pour ce jour).

| | | | |
|---|---|---|---|
| ADI XSZ | HBZ GDE | LRX BTD | SWM NLG |
| BYZ MKE | HUR GZL | MHE HCS | TCH AEI |
| COG DVH | IAS FJM | MSF HGV | UNC WIA |
| DBB CDN | IJY FPO | NUU VZJ | VIV SXF |
| DEJ CAR | JAK EJX | OQL UOU | VPG SRH |
| EAF JJV | JTU EFJ | PVZ LME | XBT YDK |
| FPU IRJ | KGL ZHU | QFH RBI | YQU KOJ |
| GSJ PGR | LRO BTW | RIU QXJ | ZHE TCS |

(1) Vérifier que lorsque les lettres à la position $i$ ($i$ étant $1, 2$ ou $3$) de deux messages-clés chiffrés sont égales, ceci est également le cas pour les lettres à la position $i+3$. Par exemple, un 'H' à la position 1, donne toujours un 'G' à la position 4. Expliquer.

(2) Dériver la permutation $\sigma_1$ qui lie une lettre $x$ à la position 1 à la lettre $\sigma_1(x)$ à la position 4 (tableau de correspondance). Par exemple $\sigma_1(\mathtt{H})=\mathtt{G}$.

(3) Décomposer cette permutation en produit de cycles.

(4) Compter la longueur de cycles. On appellera l'ensemble de ces longueurs la *caractéristique* de la permutation.

*Remarque* : Rejewski a prouvé qu'on ne peut avoir qu'un nombre pair de cycles de chaque longueur.

(5) Est-ce que la caractéristique change si on utilise une configuration différente pour le tableau des connexions ?

(6) *À la maison :* Donner les permutations $\sigma_2$ (positions $2-5$) et $\sigma_3$ (positions $3-6$).

(7) *À la maison :* Donner leurs caractéristiques.

(8) *À la maison :* (préparation du prochain TP) En supposant que pendant le chiffrement de ces 6 caractères les deux derniers rotors n'ont pas avancé, décrire une façon d'utiliser ces trois caractéristiques afin de trouver l'ordre et les réglages des rotors.

# Partie 3 - Exercices complémentaires

**Exercice 8.** *Le Chiffre ADFGVX.*

Le chiffre ADFGVX est un système de chiffrement allemand inventé par le colonel Fritz Nebel et introduit à la fin de la Première Guerre mondiale afin de sécuriser les communications radiophoniques lors de l'offensive sur Paris. Il a été cassé par le lieutenant Georges Painvin début juin 1918, donnant un avantage crucial à l'armée française.

Son originalité réside dans l'union d'une substitution inspirée du carré de Polybe et d'une transposition. Le nom du chiffre provient des coordonnées des lettres dans le carré. Les chiffres du carré de Polybe sont en effet remplacés par les lettres A, D, F, G, V et X, choisies en raison de leur codes morse très différents les uns des autres, de façon à éviter les erreurs de transmission radio.

Ici on utilise des tableaux de taille 6 permettant de coder l'ensemble des lettres de l'alphabet (non accentuées) et les 10 chiffres. Une première clé secrète consiste en la disposition des caractères dans le tableau. Une deuxième clé est représentée par une permutation permettant de mélanger le texte chiffré après application du principe de Polybe.

Par exemple, on suppose que le tableau est donné par :

| | **A** | **D** | **F** | **G** | **V** | **X** |
|---|---|---|---|---|---|---|
| **A** | c | 1 | o | f | w | j |
| **D** | y | m | t | 5 | b | 4 |
| **F** | i | 7 | a | 2 | 8 | s |
| **G** | p | 3 | 0 | q | h | x |
| **V** | k | e | u | $\ell$ | 6 | d |
| **X** | v | r | g | z | n | 9 |

Dans une première étape, on codera donc le mot `attaque` par `FF|DF|DF|FF|GG|VF|VD`. Dans une seconde étape, on va transposer (permuter) les lettres que nous venons d'obtenir selon une permutation secrète $\pi$ ayant une longueur également secrète. Supposons par exemple que la permutation $\pi$ est de longueur $n = 4$ et qu'elle est donnée par $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$. On dispose alors le texte codé en lignes successives de $n$ lettres et on complète les lignes par des caractères aléatoires (ne modifiant pas le message, `XX` ici) :

```
FFDF
DFFF
GGVF
VDXX
```

Le texte chiffré sera le résultat de la permutation par $\pi$ des colonnes :

```
FDFF
FFDF
GVGF
DXVX
```

et la lecture des caractères de haut en bas et de gauche vers la droite. Finalement on obtient le chiffré : `FFGD|DFVX|FDGV|FFFX`.

(1) Chiffrer le texte `attaquesurparisle12janvier` à l'aide du même tableau et de la permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 3 & 6 & 4 \end{pmatrix}$.

(2) Déchiffrer le texte `GFFFV FFDFF DDFXG FVDVV XFVVF GXGAD AXDGV FGVFX FFVAF FVV` qui a été chiffré à l'aide du même tableau et de la permutation $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 6 & 2 & 5 & 4 \end{pmatrix}$.

**Exercice 9.** *Chiffre de Vigenère.*
Se familiariser avec Vigenère : réaliser l'attaque « à la main ».

(1) Chiffrer à l'aide du carré de Vigenère et du mot-clé "citron" le message "*Attaquons Versailles*".

(2) Le message chiffré

`tfuefknfmtfuekaakbskaehnejmifg`

a été obtenu en utilisant le chiffre de Vigenère. Retrouver le message clair écrit en anglais. Pour vous aider, les lettres les plus fréquentes de la langue anglaise sont par ordre décroissant `e, t, a, o, i, n, s, h` et `r`.