Cryptographie – Feuille d'exercices numéro 1
Codes d'immeuble, Enigma et rappels de maths

M1 Algèbre appliquée/AMIS/DataScale/IRS/SeCReTS

Année 2023-2024

1 Exercice : Code d'immeuble et mots de passes

On cherche à trouver le code d'accès d'un immeuble. Le digicode présente k caractères ; les combinaisons valides sont composées de n caractères.

1. Combien y a-t-il de codes à 4 chiffres pour un code d'immeuble ?
2. Combien de cartes bancaires dois-je voler pour réussir avec grand probabilité à voler 1000 euros ?
3. Combien y a-t-il de codes à 4 chiffres si aucun chiffre ne peut être répété ?
4. Même question, toujours avec un code à 4 chiffres, si on rajoute deux lettres A et B.
5. Même question, toujours avec un code à 4 chiffres et avec les deux lettres A et B, si on sait que le code termine par une lettre.
6. D'après vous, combien de temps cela prendrait à un.e voleur.se pour entrer dans un immeuble avec les types de codes donnés dans les questions précédentes ?
7. Donnez plusieurs manières d'avoir un code d'immeuble sûr.
8. Supposons que le digicode présente tous les chiffres de 0 à 9. On sait que le code est composé de 4 chiffres. En appliquant du talc sur celui-ci, on peut voir que les touches les plus appuyées sont 2, 5, 8 et 9.t Combien de combinaisons faut-il essayer ?
9. Supposons que le digicode présente tous les chiffres de 0 à 9. On sait que le code est composé de 4 chiffres. En appliquant du talc sur celui-ci, on peut voir que les touches les plus appuyées sont 2, 5 et 8. Combien de combinaisons faut-il essayer ?
10. Combien de mots de passes y a-t-il à 8 chiffres ?
11. Combien de mots de passes y a-t-il à 8 caractères, incluant minuscule, majuscules, caractères spéciaux ?
12. Combien de mots de passes y a-t-il si on concatène 4 mots du dictionnaires francais, pris aléatoirement ?
13. Quels sont les caractères spéciaux que vous utilisez quand le site demande nécessairement un caractère spécial ?
14. Combien de mots de passes si vous utilisez trois premières lettres du nom du site + année d'inscription + trois caractères spéciaux pris aléatoirement ?
15. Combien d'opérations peut tester votre ordinateur personnel par seconde ? Combien de mots de passes différents faut-il afin de resister à des attaques de type brute-force pour les mots de passe ?

16. On s'identifie maintenant au syndic qui souhaite protéger l'accès à l'immeuble. Pour cela, il dispose de deux solutions concurrentes :
    (a) La première consiste en deux claviers à 10 chiffres, placés côte à côte. L'accès est autorisé une fois que la personne a saisi 4 chiffres sur le premier clavier, puis 4 chiffres sur le second.
    (b) La seconde solution propose de placer deux digicodes identiques aux précédents sur chacune des deux portes d'accès successives.

    Quelle solution vous semble la plus intéressante du point de vue sécurité ?

2 Problème : La machine Enigma

La machine Enigma est un système électromécanique de chiffrement symétrique qui fût utilisé par l'armée allemande durant la Deuxième Guerre mondiale.

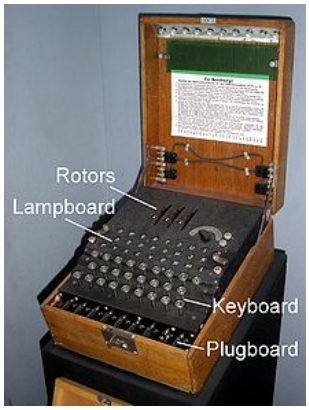

FIGURE 1 – Une machine Enigma militaire (Source : Wikipedia)

2.1 Rappels de dénombrement (cf compléments de maths discrètes)

Soit E un ensemble de n éléments distincts. On appelle *liste sans répétition* une suite ordonnée d'éléments distincts de E. Par exemple, si $E = \{1, 2, 3, 4\}$, $\mathcal{L}_1 = (1, 3, 4)$ et $\mathcal{L}_2 = (4, 3, 1)$ sont deux liste distinctes de tailles trois. On note A_n^k $(k \leq n)$ le nombre de de listes sans répétition de taille k d'éléments d'un ensemble de taille n.

1. Rappel : en énumérant pour chaque élément de la liste le nombre de choix possibles, montrer que
$$A_n^k = \frac{n!}{(n-k)!}$$
.

On appelle *combinaison* de k éléments de E tout sous-ensemble de E ayant k éléments. On note $\binom{n}{k}$ le nombre de combinaisons de k éléments d'un ensemble de taille n. Par exemple, pour $E = \{1, 2, 3, 4\}$, ses combinaisons de 3 éléments sont $\{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}$ et $\{2, 3, 4\}$ et $\binom{4}{3} = 4$

2. Rappel : monter que pour toute combinaison de taille k d'éléments de E, on peut construire $k!$ listes sans répétition de taille k.

3. Rappel : en déduire que
$$A_n^k = k!\binom{n}{k}$$
4. Rappel : en conclure que le nombre de combinaisons de k éléments d'un ensemble de taille n est
$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

2.2 Description d'Enigma

Dans la machine enigma, on commence par :
- définir la position de trois rotors (lesquels acceptent chacun 26 positions différentes), dont les connexions électriques fixent une permutation de l'alphabet ;
- définir une connexion électrique permettant de réaliser une permutation de $\{a, b, c, \ldots, z\}$ ayant 14 points fixes et 6 échanges de deux caractères (aucun caractère ne peut être présent dans deux échanges différents). Par exemple,
$$[b \leftrightarrow t, e \leftrightarrow q, g \leftrightarrow z, h \leftrightarrow i, k \leftrightarrow p, m \leftrightarrow s]$$
laisse $a, c, d, f, j, l, n, o, r, u, v, w, x$ et y inchangés et envoie b vers t et t vers b, e vers q et q vers e, etc.
- Il y a aussi un réflecteur qui est une permutation involutive de l'alphabet.
- À chaque chiffrement d'une lettre, les rotors tournent à la manière d'une montre : chaque rotor possède une position specifique, qui lorsqu'elle est atteinte, fait tourner d'un cran le rotor suivant, à la manière d'une montre (secondes, minutes)

Un exemple de machine Enigma simplifiée (limitée à 6 lettres) est représenté sur la figure **??**.

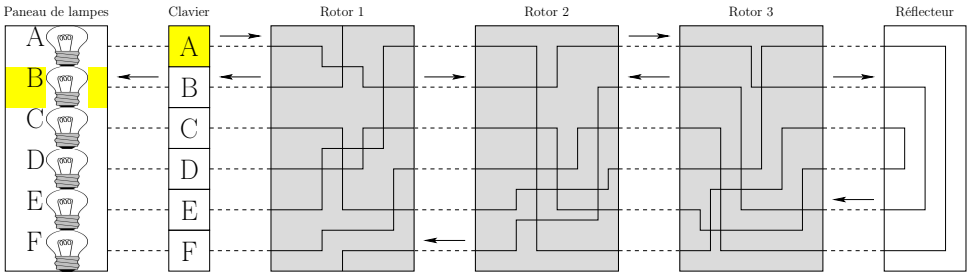

FIGURE 2 – Une machine Enigma simplifiée à 6 lettres

1. À quoi sert le réflecteur ?
2. Identifier ce qui fait partie de la machine et ce qui fait partie de la clef secrète.

2.3 Nombre de clefs dans la machine Enigma

1. Nombre de clefs
   (a) Combien existe-t-il de positions initiales des rotors ?
   (b) Combien existe-t-il de choix possibles des 12 lettres permutées ?
   (c) Plaçons ces lettres dans une table de cette forme :
   $$[\cdot \leftrightarrow \cdot, \cdot \leftrightarrow \cdot, \cdot \leftrightarrow \cdot, \cdot \leftrightarrow \cdot, \cdot \leftrightarrow \cdot, \cdot \leftrightarrow \cdot]$$
   Combien existe-t-il de façon de placer les 12 lettres dans cette table ?

(d) Parmi ces dernières, plusieurs sont équivalentes :

i. Au sein d'une même paire, $\ell_1 \leftrightarrow \ell_2$ et $\ell_2 \leftrightarrow \ell_1$ sont équivalentes. Combien faut-il éliminer de placements ?

ii. Toutes les manières d'ordonner les différentes paires sont équivalentes. Combien faut-il éliminer de placements ?

(e) Donner le nombre de clefs différentes de la machine Enigma.

2. Soit $(a_{n-1}, a_{n-2}, \ldots, a_0)_2$ un nombre encodé sur n bits (i.e. le n^e bit a_{n-1} de a est 1)

(a) En s'appuyant sur la définition de l'écriture binaire, montrer que

$$2^{n-1} \leq a$$

et que

$$a < 2^n$$

(b) En déduire que $n - 1 \leq \log_2 a < n$ et donc que $n = \lfloor \log_2 a \rfloor + 1$

(c) Combien de bits sont donc nécessaires pour représenter une clef d'Enigma ?

3. En déduire quelle est la complexité d'une recherche exhaustive sur une telle clef.

3 Quelques éléments mathématiques

3.1 Un exercice pour se mettre en jambe

$\forall p \in \mathbb{N}, \forall n \in \mathbb{N}^\star$, on définit $A_n = 2^n + p$ et d_n le pgcd de A_n et A_{n+1}.

1. Montrer que d_n divise 2^n.
2. Déterminer la parité de A_n en fonction de celle de p.
3. En déduire le pgcd de $2^{2022} + 2027$ et de $2^{2023} + 2027$.

3.2 Le groupe des permutations

1. Quel est le cardinal de l'ensemble des permutations de n éléments (noté $\mathcal{S}_n$).
2. Soient σ_1 la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$ et σ_2 la permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$. Déterminer $\sigma_1 \circ \sigma_2$.
3. Le groupe des permutations est-il abélien ?
4. Prenez plusieurs permutations arbitrairement choisies sur 7 éléments et représentez-les sous forme de graphe. Que constatez-vous ?
5. Quelles sont les permutations qui sont des involutions ?

3.3 Inversion matricielle avec coefficients dans $\mathbb{Z}/n\mathbb{Z}$

1. On se place dans $\mathbb{Z}/n\mathbb{Z}$. Quelle est la structure de cet ensemble ? rappelez comment on construit $\mathbb{Z}/n\mathbb{Z}$.
2. On regarde maintenant les matrices carrées de taille 2, à coefficients dans $\mathbb{Z}/n\mathbb{Z}$. Montrez comment on inverse une matrice et donnez sa forme. À quoi faut-il particulièrement faire attention ?
3. Donnez, pour chacune de ces matrices, son inverse, dans $\mathbb{Z}/20\mathbb{Z}$ pour la première, dans $\mathbb{Z}/17\mathbb{Z}$ pour la deuxième et dans $\mathbb{Z}/8\mathbb{Z}$ pour la troisième :

$$\begin{pmatrix} 2 & 17 \\ 3 & 5 \end{pmatrix}, \begin{pmatrix} 4 & 5 \\ 10 & 12 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 7 & 5 \end{pmatrix}$$

3.4 Euclide avec des polynômes

1. Définir la division euclidienne sur les polynômes.
2. Effectuer la division euclidienne de $X^3 + X^2 + X + 1$ par $X - 1$.
3. Déterminer deux polynômes $U(X)$ et $V(X)$ vérifiant :
   $(X^3 + X^2 + X + 1).U(X) + (X - 1).V(X) = 1$.
4. Effectuer la division euclidienne de $4X^5 + 3X^4 + X^2$ par $X^2 + X + 1$

4 Exercices complémentaires

4.1 Division euclidienne

1. Déterminer le reste dans la division euclidienne de 2011 par 11.
2. Déterminer le reste dans la division euclidienne de 2^{10} par 11.
3. Déterminer le reste dans la division euclidienne de $2^{2011} + 2011$ par 11.

4.2 Exercice : Petit théorème de Fermat

Soit p un nombre premier.

1. Montrer que, pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$. On pourra utiliser le lemme de Gauss qui explique que si a, b et c sont trois entiers, que a et b sont premiers entre eux, et que a divise bc, alors a divise c.
2. Montrer par récurrence sur $n \in \mathbb{N}$ que $n^p \equiv n\ [p]$.
3. Montrer que, si n n'est pas divisible par p, $n^{p-1} \equiv 1\ [p]$.
4. Vérifier que $2011^6 \equiv 1\ [7]$.

4.3 Euclide étendu

1. Soient a et b deux entiers, montrer que $a \wedge b = b \wedge r$
   où r est le reste de la division euclidienne de a par b.
2. Déterminer le pgcd de 442 et 495 au moyen de l'algorithme d'Euclide.
3. En effectuant une remontée de l'algorithme d'Euclide,
   déterminer $u, v \in \mathbb{Z}$ tels que $442.u + 495.v = 1$.
4. En déduire l'inverse de 442 dans $\mathbb{Z}/495\mathbb{Z}$.
5. Résoudre l'équation $442.u + 495.v = 1$ avec u et v dans $\mathbb{Z}$.

4.4 Exercice : La part du butin

Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier.

Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?