Cryptographie – Feuille d'exercices

Rappels de mathématiques

M1 Informatique – 2012-2013

1 Exercice : Code d'immeuble

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. Supposons que les caractères présents sur le digicode sont A, B, C et D et que le code n'est composé que de 2 lettres.
   - Représenter à l'aide d'un arbre tous les codes possibles ;
   - En déduire le nombre de codes possibles ?
2. Supposons que le code est composé de 3 lettres *distinctes* parmi A, B et C.
   - Représenter à l'aide d'un arbre tous les codes possibles ;
   - En déduire le nombre de codes possibles ?
3. Supposons que le code est composé de 3 lettres *distinctes* parmi A, B, C et D.
   - Représenter à l'aide d'un arbre tous les codes possibles ;
   - En déduire le nombre de codes possibles ?
4. Supposons que le digicode présente tous les chiffres de 0 à 9. On sait que le code est composé de 3 chiffres. En appliquant du talc sur celui-ci, on peut voir que les touches les plus appuyées sont 2, 5 et 8.
   - Représenter à l'aide d'un arbre tous les codes possibles ;
   - En déduire le nombre de codes possibles ?
5. Supposons que le digicode présente tous les chiffres de 0 à 9. On sait que le code est composé de 3 chiffres. En appliquant du talc sur celui-ci, on peut voir que les touches les plus appuyées sont 2, 5, 8 et 9.
   - Quel est le nombre de codes possibles ?
   - On suppose maintenant que la porte s'ouvre si on entre les bon chiffres, quel que soit leur ordre.
     - Représenter à l'aide d'un arbre les codes possibles.
     - Quel est le nombre de codes possibles ?
6. Supposons que le digicode présente tous les chiffres de 0 à 9 et les lettres A et B. On sait que le code est composé de 3 chiffres et se termine par une lettre. Quel est le nombre de codes possibles ?
7. Reprenez les questions précédentes dans le cas général.
8. On suppose qu'un attaquant met en moyenne 3 secondes pour saisir un code. Quel est, pour chacun des cas précédents, le temps d'attaque maximal nécessaire à l'ouverture de la porte si $n = 10$ et pour les cas où $k = 4, 5$ ou 6.

9. 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 (Sujet de contrôle continu 2011–2012)

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

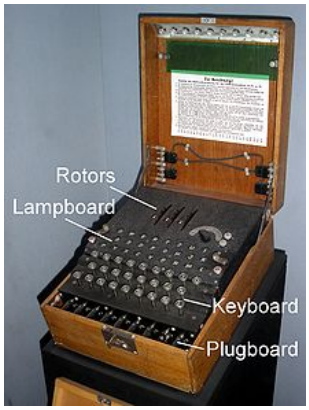

FIGURE 1 – Une machine Enigma militaire (Source : Wikipedia)

La clef secrète consiste à choisir
- la position de trois rotors (lesquels acceptent chacun 26 positions différentes) ;
- 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.

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

2.1 (Quelques résultats de dénombrement)

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.

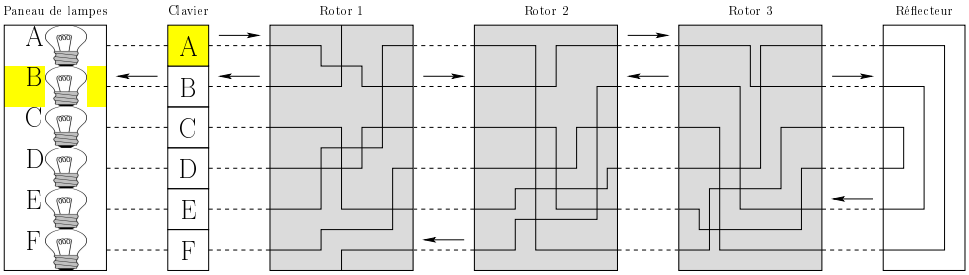

FIGURE 2 – Une machine Enigma simplifiée à 6 lettres

1. 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 $\binom{4}{3} = 4$

1. Monter que pour toute combinaisons de taille k d'éléments de E, on peut constuire $k!$ listes sans répétion de taille k (on rappelle que $0! = 1$).
2. En déduire que

$$A_n^k = k!\binom{n}{k}$$

3. 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 Application à la taille des clefs

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 (i.e. le nombre de sous-ensembles de 12 lettres parmi 26) ?
   (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) En déduire que le nombre de clefs différentes de la machine Enigma est

$$26^3 \binom{26}{12} \frac{12!}{(6!)\,2^6} = 1\ 764\ 486\ 127\ 404\ 000 \approx 1,76 \cdot 10^{15} \approx 2^{50.65}$$

2. Soit $(a)_{10} = (a_{n-1}, a_{n-2}, \ldots, a_0)_2$ un nombre de 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

   $$a < 2^n$$

   (On pourra utiliser le fait que $\sum_{i=1}^{n-1} aq^i = a\frac{1-q^n}{1-q}$)
   (b) En déduire que $n - 1 \leq \log_2 a < n$ et donc que $n = \lceil \log_2 a \rceil$
   (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 Exercice : type BAC

3.1 Préliminaires

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.

3.2 (Entrée dans le vif du sujet)

$\forall p \in \mathbb{N}, \forall n \in \mathbb{N}^\star$, 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. Justifier.
3. Déterminer la parité de d_n en fonction de celle de p.
   En déduire le pgcd de $2^{2011} + 2011$ et de $2^{2012} + 2011$.

4 Exercice : Groupes, Anneaux et Corps

1. Groupes
   (a) Quel est le cardinal de l'ensemble des permutations de n éléments (noté $\mathcal{S}_n$).
   (b) 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 $\sigma_1 \circ \sigma_2$.
   (c) Le groupe des permutations est-il abélien ?
   (d) Citer d'autres groupes.
2. Anneaux
   (a) Montrer que l'inverse de $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ est $\frac{1}{ad-bc}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$

(b) Citer d'autres anneaux.

3. Corps
   (a) Montrer que l'anneau $\mathbb{Z}/n\mathbb{Z}$ est un corps si et seulement si n est premier.
   (b) Exhiber un contre-exemple au fait que $\mathbb{Z}/4\mathbb{Z}$ soit un corps.
   (c) Donner la table de multiplication de $(\mathbb{Z}/6\mathbb{Z})^\star$ et de $(\mathbb{Z}/5\mathbb{Z})^\star$.
   (d) Citer d'autres corps.

5 Exercice : Petit théorème de Fermat

Soit p un nombre premier.

1. Montrer que, pour tout $k \in [\![1, p-1]\!]$, p divise $\binom{p}{k}$.
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 $2011^6 \equiv 1\ [7]$.

6 Exercice : Algorithme d'Euclide - Application

6.1 Avec des entiers

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 $\mathbb{Z}$.

6.2 (Avec des polynômes)

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

7 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 chinois. 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 ?