Challenge Cryptanalyse

Permutations

Une application $f : X \to Y$ est *bijective* si tout élément de Y admet un unique antécédent par f dans X, i.e. si pour tout $y \in Y$, il existe un unique $x \in X$, tel que $f(x) = y$. En notant $f^{-1}(y)$ cet unique x, on définit une application $f^{-1} : Y \to X$, appelée *inverse* de f. En particulier, pour tout $x \in X$, $f^{-1} \circ f(x) = x$ et, pour tout $y \in Y$, $f \circ f^{-1}(y) = y$.

Définition. Une *permutation* σ sur un ensemble $\mathcal{E}$ (fini ou non) est une application bijective de $\mathcal{E}$ dans $\mathcal{E}$. On note $\mathfrak{S}(\mathcal{E})$ l'ensemble des permutations de $\mathcal{E}$.

Exemple. Lors d'un chiffrage par substitution monoalphabétique, la substitution appliquée est une permutation sur l'alphabet. Pour déchiffrer, il faut appliquer la permutation inverse.

On pose $\mathbb{N}_n = \{1, \ldots, n\}$ et $\mathfrak{S}_n = \mathfrak{S}(\mathbb{N}_n)$. On observe facilement que $\mathfrak{S}_n$ contient $n!$ éléments.
Si $\mathcal{E}$ est un ensemble fini de cardinal n, quitte à numéroter ses éléments de 1 à n, on peut identifier $\mathfrak{S}(\mathcal{E})$ à $\mathfrak{S}_n$. En particulier, si $\mathcal{A} = \{a, b, \ldots, z\}$ désigne notre alphabet latin à 26 lettres, quitte à numéroter les lettres (par exemple dans l'ordre alphabétique), on peut assimiler $\mathfrak{S}(\mathcal{A})$ à $\mathfrak{S}_{26}$.

Dans la suite, on considérera toujours $\mathcal{E}$ **fini** et l'on travaillera, sans perte de généralité, avec des permutations de $\mathfrak{S}_n$.

Notation. Si $\sigma \in \mathfrak{S}_n$, on note usuellement σ sous la forme d'une table $[\sigma(1), \sigma(2), \ldots, \sigma(n)]$.

Exemple. La permutation associée au chiffrage `rot13` est :

$$[14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13]$$

Cette notation signifie que 1 est envoyé sur 14, 2 sur 15, ..., 13 sur 16, 14 sur 1, 15 sur 2, ..., 26 sur 13. Cette permutation est son propre inverse.

Remarque culturelle. $\mathfrak{S}(\mathcal{E})$ muni de la loi de composition $\circ$ forme un *groupe*, appelé *groupe symétrique* de $\mathcal{E}$.

Exemple. On note τ la permutation associée au brouilleur de la machine Enigma, α_t, β_t et γ_t les permutations associées aux trois rotors à un instant t (car les rotors tournent au cours du temps, donc les permutations associées changent) et ρ la permutation associée au réflecteur. Le chiffrage x' par la machine Enigma d'une lettre x à un instant t correspond formellement à la séquence suivante de permutations :

$$x' = \tau^{-1} \circ \alpha_t^{-1} \circ \beta_t^{-1} \circ \gamma_t^{-1} \circ \rho \circ \gamma_t \circ \beta_t \circ \alpha_t \circ \tau(x)$$

Définition. Si $x_1, \ldots, x_p$ sont p entiers distincts de $\mathbb{N}_n$, on appelle *p-cycle* (ou *cycle de longueur p*) la permutation $\sigma \in \mathfrak{S}_n$ définie par $\sigma(x_i) = x_{i+1}$, où les indices sont pris modulo p, et $\sigma(x) = x$ pour tout $x \notin \{x_1, \ldots, x_p\}$. On appelle l'ensemble $\{x_1, \ldots, x_p\}$ le *support* du cycle et l'on note généralement $\sigma = (x_1, \ldots, x_p)$.

On se convainc aisément que si σ et σ' sont deux cycles à supports disjoints, alors ils commutent : $\sigma \circ \sigma' = \sigma' \circ \sigma$.

Exemple. Le cycle $(2, 4, 3) \in \mathfrak{S}_5$ correspond à la permutation $[1, 4, 2, 3, 5]$. Il envoie 2 sur 4, 4 sur 3 et 3 sur 2. Son support est l'ensemble $\{2, 3, 4\}$. Les autres éléments de $\mathbb{N}_5$ (1 et 5) sont laissés inchangés. On remarquera que la notation utilisée n'est pas unique : $(2, 4, 3) = (3, 2, 4) = (4, 3, 2)$.

Exemple. Un chiffrage par décalage de César correspond à l'application d'une puissance (i.e. à l'itération un nombre donné de fois) du 26-cycle suivant :

$$\sigma = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26)$$

σ envoie 1 sur 2, 2 sur 3, ..., 26 sur 1, et opère donc un décalage alphabétique d'une lettre. σ^5 (i.e. sigma appliqué 5 fois de suite) correspond à un décalage de 5 lettres (*exercice :* est-ce encore un cycle ?).

Théorème. Toute permutation se décompose de façon unique en produit de cycles à supports disjoints, à l'ordre des facteurs près (car des cycles à supports disjoints commutent).

Pratique de la décomposition. Il suffit de suivre les images itérées par σ des différents éléments de $\mathcal{E}$ pour identifier les cycles. Par exemple pour la permutation $\sigma = [3, 5, 7, 8, 6, 2, 1, 4]$ de $\mathfrak{S}_8$, on a $1 \to 3 \to 7 \to 1$, $2 \to 5 \to 6 \to 2$ et $4 \to 8 \to 4$. Ainsi σ se décompose en un produit de 3 cycles : $\sigma = (1, 3, 7) \circ (2, 5, 6) \circ (4, 8)$.

La décomposition en produit de cycles du `rot13` est :

$$(1, 14)\circ(2, 15)\circ(3, 16)\circ(4, 17)\circ(5, 18)\circ(6, 19)\circ(7, 20)\circ(8, 21)\circ(9, 22)\circ(10, 23)\circ(11, 24)\circ(12, 25)\circ(13, 26)$$

Petit exercice : Soit $\sigma \in \mathfrak{S}_n$.

- ▲ Justifier qu'il existe un $k > 1$ (fini) tel que $\forall x \in \mathbb{N}_n$, $\sigma^k(x) = x$.
- ◆ Exprimer le plus petit $k > 1$ possible en fonction des tailles des cycles de la décomposition de σ.

Conjugaison. Si $\alpha, \sigma \in \mathfrak{S}_n$, on appelle conjuguée de σ par α la permutation $\sigma' = \alpha \circ \sigma \circ \alpha^{-1}$. On a alors $\sigma' \circ \alpha(x) = \alpha \circ \sigma(x)$. Ainsi, si σ envoie x sur y, σ' envoie $\alpha(x)$ sur $\alpha(y)$.