Cours

$\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}$ a inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $\text{pgcd}(a, n) = 1 \Rightarrow \mathbb{Z}/p\mathbb{Z}$ est un corps
a diviseur de 0 dans $\mathbb{Z}/n\mathbb{Z}$ ssi $\text{pgcd}(a, n) \neq 1$

Algorithme d'Euclide étendu

Cf tableaux de con dans les TD Le déroulé de l'algorithme donne si existant l'inverse et le diviseur de 0

Formules:

$$u_i = u_{i-2} - q_i \times u_{i-1}$$
$$v_i = v_{i-2} - q_i \times v_{i-1}$$

Indice de coincidence

avec n_i le nombre d'occurrences de la lettre d'indice i dans le texte

$$\text{IC} = \sum_{i=0}^{25} \frac{n_i(n_i - 1)}{n(n-1)}$$

$\text{IC(fr)} \approx 0.074$

Indice de coincidence mutuelle

$$\text{ICM} = \sum_{i=0}^{25} \frac{m_i n_i}{nm}$$

Corrélation de Pearson

$$\rho_{X,Y} = \frac{\sum_i \left(X_i - \overline{X}\right)\left(Y_i - \overline{Y}\right)}{\sqrt{\sum_i \left(X_i - \overline{X}\right)^2}\sqrt{\sum_i \left(X_i - \overline{X}\right)^2}}$$

Chiffrement parfait

$\mathcal{P}$ et $\mathcal{K}$ les alphabets clairs et chiffrés.
$\mathcal{K}$ l'ensemble des clefs possibles.
$K \in \mathcal{K} : e_K : P \to C$ et $d_K : C \to P$ avec $\forall x \in \mathcal{P}, d_K(e_K(x)) = x$.
Les applications e_K et d_K nécessitent la connaissance complète de K pour être définies.

Supposons qu'un cryptosystème vérifie $|\mathcal{K}| = |\mathcal{P}| = |\mathcal{C}|$.
Alors il sera un chiffrement parfait ssi on a

- Toutes les clefs sont utilisées avec la même probabilité
- Pour tout couple $(m, c) \in \mathcal{P} \times \mathcal{C}$ il existe une unique clef k telle que $e_k(m) = c$.

Méthodes

Algorithme d'euclide

$$a = b \times m_1 + r_1$$
$$b = r_1 \times m_2 + r_2$$
$$\dots$$
$$r_n = 0$$

pgcd(a,b) $\text{alors } \text{pgcd}(a,b) = r_{n-1}$

Formule rapide pour l'ordre

$\text{ord}(a) = \frac{n}{\text{pgcd}(a,n)}$

$E^\times =$ ensemble des éléments inversibles

RSA

Principe

Chiffrement asymétrique. Soit p, q deux nombres premiers. $n = pq$. On choisit $e, d \in \mathbb{Z}/n\mathbb{Z}$ tels que $ed = 1 \bmod \varphi(n)$. On a $\varphi(n) = \varphi(q)\varphi(q) = (p-1)(q-1)$

Clé publique: (n, e) Clé privée: d

Bob peut chiffrer un message $m \in \mathbb{Z}/n\mathbb{Z}^\times$ avec $f : m \to m^e \bmod n$

Alice peut déchiffrer un message $c \in \mathbb{Z}/n\mathbb{Z}^\times$ avec $f : c \to c^d \bmod n$

Th des restes chinois

Soit p et q premiers entre eux. Alors Z/pqZ est isomorphe à Z/pZ times Z/qZ