Notions de probabilité

Notation : $\mathcal{X}$ un espace d'événements, X une distribution de probabilités sur $\mathcal{X}$ et $Pr_{\mathcal{X}}(x)$ la probabilité d'un événement x suivant X.

Soient X et Y deux ensembles d'événements différents.
La probabilité mutuelle $Pr_{(\mathcal{X},\mathcal{Y})}(x, y)$: probabilité que x et y soient réalisés simultanément.
La probabilité conditionnelle $Pr_{\mathcal{X}}(x|y)$: probabilité de x sachant que y est réalisé.

$$Pr(x, y)_{(\mathcal{X},\mathcal{Y})} = Pr_{\mathcal{X}}(x|y)Pr_{\mathcal{Y}}(y)$$

Th.: (Théorème de Bayes) Si $Pr_{\mathcal{Y}}(y) > 0$ alors

$$Pr_{\mathcal{X}}(x|y) = \frac{Pr_{\mathcal{X}}(x)Pr_{\mathcal{Y}}(y|x)}{Pr_{\mathcal{Y}}(y)}$$

cor.: Deux distributions X et Y sont indépendantes si et seulement si

$$Pr_{\mathcal{X}}(x|y) = Pr_{\mathcal{X}}(x), \forall x \in \mathcal{X}, \forall y \in \mathcal{Y}$$

Probabilité et cryptographie

$C(k) = \{e_k(x), x \in \mathcal{P}\}$

Probabilité d'avoir un texte chiffré y :

$$Pr_{\mathcal{C}}(y) = \Sigma_{k/y \in C(k)} Pr_{\mathcal{K}}(k) Pr_{\mathcal{P}}(d_k(y))$$

Probabilité d'avoir un texte chiffré y sachant que le texte clair est x :

$$Pr_{\mathcal{C}}(y|x) = \Sigma_{k/x \in d_k(y)} Pr_{\mathcal{K}}(k)$$

Probabilité d'avoir un texte clair x sachant que le texte chiffré est y :

$$Pr_{\mathcal{P}}(x|y) = \frac{Pr_{\mathcal{P}}(x) Pr_{\mathcal{C}}(y|x)}{Pr_{\mathcal{C}}(y)}$$

Un système cryptographique assure une confidentialité parfaite si

$$\forall x \in \mathcal{P}, \forall y \in \mathcal{C}, Pr_{\mathcal{P}}(x|y) = Pr_{\mathcal{P}}(x)$$

Probabilité et cryptographie (suite)

Th.: Soit le système cryptographique $S = \{\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D}\}$, $|\mathcal{P}|$=$|\mathcal{C}|$=$|\mathcal{K}|$. S assure une confidentialité parfaite si et seulement si
$\forall k \in \mathcal{K}, Pr_{\mathcal{K}}(k) = \frac{1}{|\mathcal{K}|}$ et
$\forall x \in \mathcal{P}, \forall y \in \mathcal{C}, \exists! k \in \mathcal{K} / e_k(x) = y$.

Exemple : Soient $\mathcal{P} = \{a, b\}$ avec $Pr_{\mathcal{P}}(a) = \frac{1}{4}$ et $Pr_{\mathcal{P}}(b) = \frac{3}{4}$; $\mathcal{K} = \{k_1, k_2, k_3\}$ et $Pr_{\mathcal{K}}(k_1) = \frac{1}{2}$, $Pr_{\mathcal{K}}(k_2) = \frac{1}{4}$, $Pr_{\mathcal{K}}(k_3) = \frac{1}{4}$; $\mathcal{C} = \{1, 2, 3, 4\}$.

$e_k(x)$	k_1	k_2	k_3
a	1	2	3
b	2	3	4

Calculer $\forall x \in \mathcal{P}, \forall y \in \mathcal{C}, Pr(x|y)$?