Cours 2. Entropie. Applications à la cryptographie.

A. Désilles

30 mars 2009

Résumé

Résumé

Résumé

Résumé

Résumé

Rappels : Modèle de communication

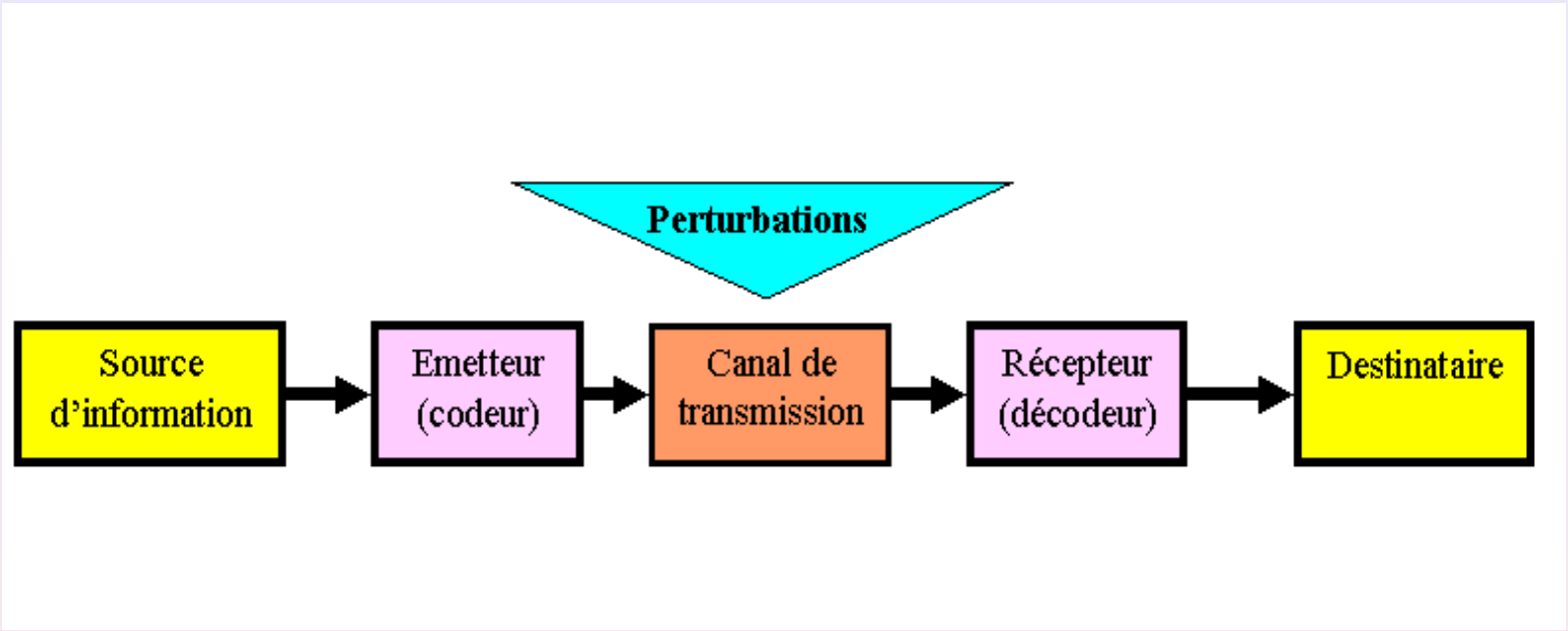

Figure: Paradigme de Shannon

Rappels : Représentation mathématique d'une source

- Une source d'information peut être :
  - un texte
  - un son
  - une image
- Elle est représentée par un ensemble fini d'éléments, appelé alphabet.
- Les éléments de l'alphabet sont appelés symboles (caractères, lettres).
- Toute séquence finie d'éléments d'alphabet est appelée mot (message).

Rappels : Représentation mathématique d'une source

- Une source d'information peut être :
  - un texte
  - un son
  - une image
- Elle est représentée par un ensemble fini d'éléments, appelé alphabet.
- Les éléments de l'alphabet sont appelés symboles (caractères, lettres).
- Toute séquence finie d'éléments d'alphabet est appelée mot (message).

Rappels : Représentation mathématique d'une source

- Une source d'information peut être :
  - un texte
  - un son
  - une image
- Elle est représentée par un ensemble fini d'éléments, appelé alphabet.
- Les éléments de l'alphabet sont appelés symboles (caractères, lettres).
- Toute séquence finie d'éléments d'alphabet est appelée mot (message).

Rappels : Représentation mathématique d'une source

- Une source d'information peut être :
  - un texte
  - un son
  - une image
- Elle est représentée par un ensemble fini d'éléments, appelé alphabet.
- Les éléments de l'alphabet sont appelés symboles (caractères, lettres).
- Toute séquence finie d'éléments d'alphabet est appelée mot (message).

Rappels : Représentation mathématique d'une source

- Une source d'information peut être :
  - un texte
  - un son
  - une image
- Elle est représentée par un ensemble fini d'éléments, appelé alphabet.
- Les éléments de l'alphabet sont appelés symboles (caractères, lettres).
- Toute séquence finie d'éléments d'alphabet est appelée mot (message).

Rappels : Représentation mathématique d'une source

- Une source d'information peut être :
  - un texte
  - un son
  - une image
- Elle est représentée par un ensemble fini d'éléments, appelé alphabet.
- Les éléments de l'alphabet sont appelés symboles (caractères, lettres).
- Toute séquence finie d'éléments d'alphabet est appelée mot (message).

Rappels : Représentation mathématique d'une source

- Une source d'information peut être :
  - un texte
  - un son
  - une image
- Elle est représentée par un ensemble fini d'éléments, appelé alphabet.
- Les éléments de l'alphabet sont appelés symboles (caractères, lettres).
- Toute séquence finie d'éléments d'alphabet est appelée mot (message).

Modèle d'une source d'information

Une source d'information X est décrite par un couple (Ω_X, P_X) où Ω_X est un alphabet fini et P_X est une distribution de probabilités sur Ω_X.

Rappels : Information propre.

Définition

Soient $\Omega = \{\omega_1, \ldots, \omega_m\}$ un alphabet discret et X la variable aléatoire associée. Pour tout événement $A \subset \Omega$ la quantité d'information propre de A est définie par

$$h(A) = -\log_2(P(A)).$$

Entropie d'une source

Soient $\Omega_X = \{x_1, \ldots, x_m\}$ l'alphabet fini d'une source et X la variable aléatoire associée t.q. $P[\omega_i] = p_i, \quad i = 1, \ldots, m$. On appelle **entropie** ou encore **quantité moyenne d'information** de la source la quantité

$$H(X) = H(p_1, p_2, \ldots, p_n) = E[h(x)] = -\sum_{i=1}^{m} p_i \log_2(p_i)$$

L'unité de mesure de cette quantité est le "bit par symbole".

Interprétations

- **Entropie comme mesure d'information**
- Entropie comme mesure de nombre de bits pour le codage

Interprétations

- **Entropie comme mesure d'information**
- **Entropie comme mesure de nombre de bits pour le codage**

Entropie d'une source. Propriétés

Soit X une source d'alphabet $\Omega_X = \{x_i\}_{i=1}^n$et de de distribution de probabilité P donnée $P[X = x_i] = p_i, \quad i = 1, \ldots, n$. Notons $H(p_1, \ldots, p_n)$ sa fonction d'entropie. Alors

- **Positivité**

$$H(p_1, p_2, \ldots, p_n) \geq 0.$$

  L'égalité a lieu uniquement si l'une des probabilités p_i est égale à 1 et les autres sont nulles.

- **Propriété de maximum**

$$H(p_1, p_2, \ldots, p_n) \leq log(n)$$

  et l'égalité a lieu si et seulement si $\forall i = 1, \ldots, n, \quad p_i = \frac{1}{n}$.

- A retenir. L'entropie est maximale lorsque la distribution des probabilités est uniforme : tous les symboles sont équiprobables.

Entropie d'une source. Propriétés

Soit X une source d'alphabet $\Omega_X = \{x_i\}_{i=1}^n$et de de distribution de probabilité P donnée $P[X = x_i] = p_i, \quad i = 1, \ldots, n$. Notons $H(p_1, \ldots, p_n)$ sa fonction d'entropie. Alors

- **Positivité**

$$H(p_1, p_2, \ldots, p_n) \geq 0.$$

  L'égalité a lieu uniquement si l'une des probabilités p_i est égale à 1 et les autres sont nulles.

- **Propriété de maximum**

$$H(p_1, p_2, \ldots, p_n) \leq log(n)$$

  et l'égalité a lieu si et seulement si $\forall i = 1, \ldots, n, \quad p_i = \frac{1}{n}$.

- A retenir. L'entropie est maximale lorsque la distribution des probabilités est uniforme : tous les symboles sont équiprobables.

Entropie d'une source. Propriétés

Soit X une source d'alphabet $\Omega_X = \{x_i\}_{i=1}^n$et de de distribution de probabilité P donnée $P[X = x_i] = p_i, \quad i = 1, \ldots, n$. Notons $H(p_1, \ldots, p_n)$ sa fonction d'entropie. Alors

- **Positivité**

$$H(p_1, p_2, \ldots, p_n) \geq 0.$$

  L'égalité a lieu uniquement si l'une des probabilités p_i est égale à 1 et les autres sont nulles.

- **Propriété de maximum**

$$H(p_1, p_2, \ldots, p_n) \leq log(n)$$

  et l'égalité a lieu si et seulement si $\forall i = 1, \ldots, n, \quad p_i = \frac{1}{n}$.

- A retenir. L'entropie est maximale lorsque la distribution des probabilités est uniforme : tous les symboles sont équiprobables.

Entropie conjointe

Définition

Soient $X = \{x_i\}_{i=1}^{n}$ et $Y = \{y_j\}_{j=1}^{m}$ deux variables aléatoires discrètes définies sur un même univers.
Soit $P(i,j) = P[X = x_i \text{ et } Y = y_j]$ leur distribution conjointe.
Alors **l'entropie conjointe de X et Y** est définie par

$$H(X,Y) = -\sum_{i=1}^{n}\sum_{j=1}^{n} P(i,j)\log(P(i,j)).$$

Étude des associations de symboles d'une source

Soit une source S d'alphabet $\Omega = \{a, e, o, c, p, r, t\}$. Supposons que tous les symboles soient équiprobables. L'entropie de cette source est alors

$$H(S) = \log_2(7) \simeq 2.80 \text{ bits par symbole.}$$

Pour coder chaque symbole d'un message on ne peut pas utiliser en moyenne moins de 2.80 bits par symbole.

Étude des associations de symboles d'une source

Soit une source S d'alphabet $\Omega = \{a, e, o, c, p, r, t\}$. Supposons que tous les symboles soient équiprobables. L'entropie de cette source est alors

$$H(S) = \log_2(7) \simeq 2.80 \text{ bits par symbole.}$$

Pour coder chaque symbole d'un message on ne peut pas utiliser en moyenne moins de 2.80 bits par symbole.

Étude des associations de symboles d'une source

On peut étudier les syllabes formées d'une consonne et d'une voyelle.
Supposons que les probabilités sont données par le tableau suivant :

$Y \backslash X$	a	e	o	$P_Y(y)$
c	0.05	0.05	0.1	0.2
p	0.1	0.15	0.05	0.3
r	0.05	0.1	0.1	0.25
t	0.15	0.05	0.05	0.25
$P_X(x)$	0.35	0.35	0.3	

L'entropie conjointe de X et Y est alors

$$H(X,Y) =$$

Étude des associations de symboles d'une source

On peut étudier les syllabes formées d'une consonne et d'une voyelle.
Supposons que les probabilités sont données par le tableau suivant :

$Y \backslash X$	a	e	o	$P_Y(y)$
c	0.05	0.05	0.1	0.2
p	0.1	0.15	0.05	0.3
r	0.05	0.1	0.1	0.25
t	0.15	0.05	0.05	0.25
$P_X(x)$	0.35	0.35	0.3	

L'entropie conjointe de X et Y est alors

$$H(X, Y) =$$

Étude des associations de symboles d'une source

On peut étudier les syllabes formées d'une consonne et d'une voyelle.
Supposons que les probabilités sont données par le tableau suivant :

$Y \backslash X$	a	e	o	$P_Y(y)$
c	0.05	0.05	0.1	0.2
p	0.1	0.15	0.05	0.3
r	0.05	0.1	0.1	0.25
t	0.15	0.05	0.05	0.25
$P_X(x)$	0.35	0.35	0.3	

L'entropie conjointe de X et Y est alors

$$H(X,Y) = -6 \cdot 0.05 \log(0.05)$$

Étude des associations de symboles d'une source

On peut étudier les syllabes formées d'une consonne et d'une voyelle.
Supposons que les probabilités sont données par le tableau suivant :

$Y \backslash X$	a	e	o	$P_Y(y)$
c	0.05	0.05	0.1	0.2
p	0.1	0.15	0.05	0.3
r	0.05	0.1	0.1	0.25
t	0.15	0.05	0.05	0.25
$P_X(x)$	0.35	0.35	0.3	

L'entropie conjointe de X et Y est alors

$$H(X,Y) = -6 \cdot 0.05 \log(0.05) - 4 \cdot 0.1 \log(0.1)$$

Étude des associations de symboles d'une source

On peut étudier les syllabes formées d'une consonne et d'une voyelle.
Supposons que les probabilités sont données par le tableau suivant :

$Y \backslash X$	a	e	o	$P_Y(y)$
c	0.05	0.05	0.1	0.2
p	0.1	0.15	0.05	0.3
r	0.05	0.1	0.1	0.25
t	0.15	0.05	0.05	0.25
$P_X(x)$	0.35	0.35	0.3	

L'entropie conjointe de X et Y est alors

$$H(X,Y) = -6 \cdot 0.05 \log(0.05) - 4 \cdot 0.1 \log(0.1) - 2 \cdot 0.15 \log(0.15)$$

Étude des associations de symboles d'une source

On peut étudier les syllabes formées d'une consonne et d'une voyelle.
Supposons que les probabilités sont données par le tableau suivant :

$Y \backslash X$	a	e	o	$P_Y(y)$
c	0.05	0.05	0.1	0.2
p	0.1	0.15	0.05	0.3
r	0.05	0.1	0.1	0.25
t	0.15	0.05	0.05	0.25
$P_X(x)$	0.35	0.35	0.3	

L'entropie conjointe de X et Y est alors

$$H(X,Y) = -6 \cdot 0.05 \log(0.05) - 4 \cdot 0.1 \log(0.1) - 2 \cdot 0.15 \log(0.15) \simeq 3.44$$

Pour coder chaque couple il suffirait en moyenne 3.44 bits par couple au lieu de $2 \times 2.80 = 5.6$ bits, si l'on codait chaque symbole du couple séparément.

Entropie conditionnelle moyenne

Définition

Soient $X = \{x_i\}_{i=1}^{n}$ et $Y = \{y_j\}_{j=1}^{m}$ deux variables aléatoires discrètes définies sur un même univers.

Soit $P(i,j) = P[X = x_i \text{et } Y = y_j]$ leur distribution conjointe.

Posons $P(i|j) = P[X = x_i | Y = y_j] = \dfrac{P(i,j)}{P[Y = y_j]}$.

Alors l'**entropie conditionnelle moyenne** de X sachant Y est définie par

$$H(X|Y) = -\sum_{i=1}^{n}\sum_{j=1}^{m} P(i,j)\log(P(i|j)).$$

Propriétés

1. **Additivité.**

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$$

2. $$H(X,Y) \geq 0, \quad H(X|Y) \geq 0$$

   L'entropie conjointe $H(X,Y)$ est nulle ssi une seule des combinaisons (x_i, y_j) est possible. L'entropie conditionnelle moyenne $H(X|Y)$ est nulle ssi X est une fonction de Y.

3. $$H(X,Y) \geq \max(H(X), H(Y))$$

4. $$H(X,Y) \leq H(X) + H(Y) \leq 2H(X+Y)$$

Propriétés

1. **Additivité.**

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$$

2. $$H(X,Y) \geq 0, \quad H(X|Y) \geq 0$$

   L'entropie conjointe $H(X,Y)$ est nulle ssi une seule des combinaisons (x_i, y_j) est possible. L'entropie conditionnelle moyenne $H(X|Y)$ est nulle ssi X est une fonction de Y.

3. $$H(X,Y) \geq \max(H(X), H(Y))$$

4. $$H(X,Y) \leq H(X) + H(Y) \leq 2H(X+Y)$$

Propriétés

1. **Additivité.**

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$$

2. $$H(X,Y) \geq 0, \quad H(X|Y) \geq 0$$

   L'entropie conjointe $H(X,Y)$ est nulle ssi une seule des combinaisons (x_i, y_j) est possible. L'entropie conditionnelle moyenne $H(X|Y)$ est nulle ssi X est une fonction de Y.

3. $$H(X,Y) \geq \max(H(X), H(Y))$$

4. $$H(X,Y) \leq H(X) + H(Y) \leq 2H(X+Y)$$

Propriétés

1. **Additivité.**

$$H(X,Y) = H(X) + H(Y|X) = H(Y) + H(X|Y)$$

2. $$H(X,Y) \geq 0, \quad H(X|Y) \geq 0$$

   L'entropie conjointe $H(X,Y)$ est nulle ssi une seule des combinaisons (x_i, y_j) est possible. L'entropie conditionnelle moyenne $H(X|Y)$ est nulle ssi X est une fonction de Y.

3. $$H(X,Y) \geq \max(H(X), H(Y))$$

4. $$H(X,Y) \leq H(X) + H(Y) \leq 2H(X+Y)$$

Information mutuelle moyenne

Définition

Soient $X = \{x_i\}_{i=1}^n$ et $Y = \{y_j\}_{j=1}^m$ deux variables aléatoires discrètes définies sur un même univers. Soit $P(i,j) = P[X = x_i \text{et } Y = y_j]$ leur distribution conjointe. L'information mutuelle moyenne de X et Y est définie par

$$I(X;Y) = \sum_{i=1}^{n}\sum_{j=1}^{m} P(i,j)\log\left(\frac{P(i,j)}{P(x_i)P(y_j)}\right).$$

Interprétation

À partir des définitions données ci-dessus on déduit facilement ces relations importantes :

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y)$$

Dans le cas où les variables X et Y représentent respectivement le message émis et le message reçu par le destinataire, cette relation signifie que l'information mutuelle moyenne est égale à :

- l'information émise $H(X)$, diminuée de l'incertitude sur le symbole x émis quand le symbole y reçu est connu, $H(X|Y)$;
- et de façon symétrique, l'information reçue, diminuée de l'incertitude sur le symbole reçu y quand le symbole émis x est connu, $H(Y|X)$.

Interprétation

À partir des définitions données ci-dessus on déduit facilement ces relations importantes :

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y)$$

Dans le cas où les variables X et Y représentent respectivement le message émis et le message reçu par le destinataire, cette relation signifie que l'information mutuelle moyenne est égale à :

- l'information émise $H(X)$, diminuée de l'incertitude sur le symbole x émis quand le symbole y reçu est connu, $H(X|Y)$;
- et de façon symétrique, l'information reçue, diminuée de l'incertitude sur le symbole reçu y quand le symbole émis x est connu, $H(Y|X)$.

Interprétation

À partir des définitions données ci-dessus on déduit facilement ces relations importantes :

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y)$$

Dans le cas où les variables X et Y représentent respectivement le message émis et le message reçu par le destinataire, cette relation signifie que l'information mutuelle moyenne est égale à :

- l'information émise $H(X)$, diminuée de l'incertitude sur le symbole x émis quand le symbole y reçu est connu, $H(X|Y)$;
- et de façon symétrique, l'information reçue, diminuée de l'incertitude sur le symbole reçu y quand le symbole émis x est connu, $H(Y|X)$.

Interprétation

À partir des définitions données ci-dessus on déduit facilement ces relations importantes :

$$I(X;Y) = H(X) - H(X|Y) = H(Y) - H(Y|X) = H(X) + H(Y) - H(X,Y)$$

Dans le cas où les variables X et Y représentent respectivement le message émis et le message reçu par le destinataire, cette relation signifie que l'information mutuelle moyenne est égale à :

- l'information émise $H(X)$, diminuée de l'incertitude sur le symbole x émis quand le symbole y reçu est connu, $H(X|Y)$;
- et de façon symétrique, l'information reçue, diminuée de l'incertitude sur le symbole reçu y quand le symbole émis x est connu, $H(Y|X)$.

Modèle complet d'un canal de communication

Un canal de transmission **stationnaire et sans mémoire** peut être modélisé par le triplet $(X, Y, P(Y|X)$ où

- X est la variable aléatoire de la source
- Y est la variable aléatoire du récepteur
- $P(Y|X)$ est appelée matrice de transition et est définie par

$$p_{i|j} = P[y_j|\, x_i],\ i = 1, \ldots, n,\ j = 1, \ldots, m$$

Cette matrice décrit les propriétés du bruit dans le canal.

- Le terme "**sans mémoire**" signifie que la réception à tout instant d'un symbole Y ne dépend que du symbole émis X. En particulier, chaque symbole reçu est indépendant des symboles reçus précédemment.
- Le terme "**stationnaire**" signifie que les caractéristiques probabilistes du bruit sont indépendantes du temps. Ainsi, à tout instant de transmission, cette matrice est la même.

Modèle complet d'un canal de communication

Un canal de transmission **stationnaire et sans mémoire** peut être modélisé par le triplet $(X, Y, P(Y|X)$ où

- X est la variable aléatoire de la source
- Y est la variable aléatoire du récepteur
- $P(Y|X)$ est appelée matrice de transition et est définie par

$$p_{i|j} = P[y_j|\, x_i],\ i = 1, \ldots, n,\ j = 1, \ldots, m$$

Cette matrice décrit les propriétés du bruit dans le canal.

- Le terme "**sans mémoire**" signifie que la réception à tout instant d'un symbole Y ne dépend que du symbole émis X. En particulier, chaque symbole reçu est indépendant des symboles reçus précédemment.
- Le terme "**stationnaire**" signifie que les caractéristiques probabilistes du bruit sont indépendantes du temps. Ainsi, à tout instant de transmission, cette matrice est la même.

Modèle complet d'un canal de communication

Un canal de transmission **stationnaire et sans mémoire** peut être modélisé par le triplet $(X, Y, P(Y|X)$ où

- X est la variable aléatoire de la source
- Y est la variable aléatoire du récepteur
- $P(Y|X)$ est appelée matrice de transition et est définie par

$$p_{i|j} = P[y_j|\, x_i],\ i = 1, \ldots, n,\ j = 1, \ldots, m$$

Cette matrice décrit les propriétés du bruit dans le canal.

- Le terme **"sans mémoire"** signifie que la réception à tout instant d'un symbole Y ne dépend que du symbole émis X. En particulier, chaque symbole reçu est indépendant des symboles reçus précédemment.
- Le terme **"stationnaire"** signifie que les caractéristiques probabilistes du bruit sont indépendantes du temps. Ainsi, à tout instant de transmission, cette matrice est la même.

Modèle complet d'un canal de communication

Un canal de transmission **stationnaire et sans mémoire** peut être modélisé par le triplet $(X, Y, P(Y|X)$ où

- X est la variable aléatoire de la source
- Y est la variable aléatoire du récepteur
- $P(Y|X)$ est appelée matrice de transition et est définie par

$$p_{i|j} = P[y_j|\, x_i],\ i = 1, \ldots, n,\ j = 1, \ldots, m$$

Cette matrice décrit les propriétés du bruit dans le canal.

- Le terme **"sans mémoire"** signifie que la réception à tout instant d'un symbole Y ne dépend que du symbole émis X. En particulier, chaque symbole reçu est indépendant des symboles reçus précédemment.
- Le terme **"stationnaire"** signifie que les caractéristiques probabilistes du bruit sont indépendantes du temps. Ainsi, à tout instant de transmission, cette matrice est la même.

Modèle complet d'un canal de communication

Un canal de transmission **stationnaire et sans mémoire** peut être modélisé par le triplet $(X, Y, P(Y|X)$ où

- X est la variable aléatoire de la source
- Y est la variable aléatoire du récepteur
- $P(Y|X)$ est appelée matrice de transition et est définie par

$$p_{i|j} = P[y_j|\, x_i],\ i = 1, \ldots, n,\ j = 1, \ldots, m$$

Cette matrice décrit les propriétés du bruit dans le canal.

- Le terme **"sans mémoire"** signifie que la réception à tout instant d'un symbole Y ne dépend que du symbole émis X. En particulier, chaque symbole reçu est indépendant des symboles reçus précédemment.
- Le terme **"stationnaire"** signifie que les caractéristiques probabilistes du bruit sont indépendantes du temps. Ainsi, à tout instant de transmission, cette matrice est la même.

On peut associer à un système de communication "source - canal - récepteur" différentes entropies :

- $H(X)$. **L'entropie de la source** Elle représente l'information moyenne par symbole de la source ou encore la difficulté moyenne de prédire le symbole émis.
- $H(Y)$. **L'entropie du récepteur** Elle représente l'information moyenne par symbole reçu ou encore la difficulté moyenne de prédire le symbole reçu.
- $H(X, Y)$. **L'entropie conjointe "source-récepteur"** Elle représente l'incertitude moyenne du système de communication dans son ensemble ou encore la quantité de l'information moyenne par paire "symbole émis - symbole reçu".

On peut associer à un système de communication "source - canal - récepteur" différentes entropies :

- $H(X)$. **L'entropie de la source** Elle représente l'information moyenne par symbole de la source ou encore la difficulté moyenne de prédire le symbole émis.
- $H(Y)$. **L'entropie du récepteur** Elle représente l'information moyenne par symbole reçu ou encore la difficulté moyenne de prédire le symbole reçu.
- $H(X, Y)$. **L'entropie conjointe "source-récepteur"** Elle représente l'incertitude moyenne du système de communication dans son ensemble ou encore la quantité de l'information moyenne par paire "symbole émis - symbole reçu".

On peut associer à un système de communication "source - canal - récepteur" différentes entropies :

- $H(X)$. **L'entropie de la source** Elle représente l'information moyenne par symbole de la source ou encore la difficulté moyenne de prédire le symbole émis.
- $H(Y)$. **L'entropie du récepteur** Elle représente l'information moyenne par symbole reçu ou encore la difficulté moyenne de prédire le symbole reçu.
- $H(X, Y)$. **L'entropie conjointe "source-récepteur"** Elle représente l'incertitude moyenne du système de communication dans son ensemble ou encore la quantité de l'information moyenne par paire "symbole émis - symbole reçu".

On peut associer à un système de communication "source - canal - récepteur" différentes entropies :

- $H(X|Y)$. **L'entropie conditionnelle de la source, sachant le symbole reçu** Elle représente l'incertitude moyenne sur le symbole émis lorsqu'on connaît le symbole reçu.
- $H(Y|X)$. **L'entropie conditionnelle du récepteur, sachant le symbole émis** Elle représente l'incertitude moyenne sur le symbole reçu lorsqu'on connaît le symbole émis.
- $I(X;Y)$. **L'information mutuelle moyenne** Elle représente la quantité moyenne d'information par symbole transmise à travers le canal.

On peut associer à un système de communication "source - canal - récepteur" différentes entropies :

- $H(X|Y)$. **L'entropie conditionnelle de la source, sachant le symbole reçu** Elle représente l'incertitude moyenne sur le symbole émis lorsqu'on connaît le symbole reçu.
- $H(Y|X)$. **L'entropie conditionnelle du récepteur, sachant le symbole émis** Elle représente l'incertitude moyenne sur le symbole reçu lorsqu'on connaît le symbole émis.
- $I(X;Y)$. **L'information mutuelle moyenne** Elle représente la quantité moyenne d'information par symbole transmise à travers le canal.

On peut associer à un système de communication "source - canal - récepteur" différentes entropies :

- $H(X|Y)$. **L'entropie conditionnelle de la source, sachant le symbole reçu** Elle représente l'incertitude moyenne sur le symbole émis lorsqu'on connaît le symbole reçu.
- $H(Y|X)$. **L'entropie conditionnelle du récepteur, sachant le symbole émis** Elle représente l'incertitude moyenne sur le symbole reçu lorsqu'on connaît le symbole émis.
- $I(X;Y)$. **L'information mutuelle moyenne** Elle représente la quantité moyenne d'information par symbole transmise à travers le canal.

Cryptographie. Vocabulaire.

- La **cryptographie** est une science qui étudie les méthodes permettant de transmettre des messages de façon confidentielle.
- **message clair** : un ensemble de données (texte, image,...) que l'on souhaite transmettre.
- Le **chiffrement** est un procédé permettant de transformer le message clair de telle sorte qu'il soit incompréhensible par qui que ce soit d'autre que l'auteur du message et le destinataire.
- Le **chiffré** est le résultat du chiffrement.
- Le **déchiffrement** est le procédé permettant de retrouver le message clair à partir du chiffré.
- La **clé** de chiffrement est un paramètre qui est utilisé dans le procédé de chiffrement ou déchiffrement.

Cryptographie. Vocabulaire.

- La **cryptographie** est une science qui étudie les méthodes permettant de transmettre des messages de façon confidentielle.
- **message clair** : un ensemble de données (texte, image,...) que l'on souhaite transmettre.
- Le **chiffrement** est un procédé permettant de transformer le message clair de telle sorte qu'il soit incompréhensible par qui que ce soit d'autre que l'auteur du message et le destinataire.
- Le **chiffré** est le résultat du chiffrement.
- Le **déchiffrement** est le procédé permettant de retrouver le message clair à partir du chiffré.
- La clé de chiffrement est un paramètre qui est utilisé dans le procédé de chiffrement ou déchiffrement.

Cryptographie. Vocabulaire.

- La **cryptographie** est une science qui étudie les méthodes permettant de transmettre des messages de façon confidentielle.
- **message clair** : un ensemble de données (texte, image,...) que l'on souhaite transmettre.
- Le **chiffrement** est un procédé permettant de transformer le message clair de telle sorte qu'il soit incompréhensible par qui que ce soit d'autre que l'auteur du message et le destinataire.
- Le **chiffré** est le résultat du chiffrement.
- Le **déchiffrement** est le procédé permettant de retrouver le message clair à partir du chiffré.
- La **clé** de chiffrement est un paramètre qui est utilisé dans le procédé de chiffrement ou déchiffrement.

Cryptographie. Vocabulaire.

- La **cryptographie** est une science qui étudie les méthodes permettant de transmettre des messages de façon confidentielle.
- **message clair** : un ensemble de données (texte, image,...) que l'on souhaite transmettre.
- Le **chiffrement** est un procédé permettant de transformer le message clair de telle sorte qu'il soit incompréhensible par qui que ce soit d'autre que l'auteur du message et le destinataire.
- Le **chiffré** est le résultat du chiffrement.
- Le **déchiffrement** est le procédé permettant de retrouver le message clair à partir du chiffré.
- La **clé** de chiffrement est un paramètre qui est utilisé dans le procédé de chiffrement ou déchiffrement.

Cryptographie. Vocabulaire.

- La **cryptographie** est une science qui étudie les méthodes permettant de transmettre des messages de façon confidentielle.
- **message clair** : un ensemble de données (texte, image,...) que l'on souhaite transmettre.
- Le **chiffrement** est un procédé permettant de transformer le message clair de telle sorte qu'il soit incompréhensible par qui que ce soit d'autre que l'auteur du message et le destinataire.
- Le **chiffré** est le résultat du chiffrement.
- Le **déchiffrement** est le procédé permettant de retrouver le message clair à partir du chiffré.
- La **clé** de chiffrement est un paramètre qui est utilisé dans le procédé de chiffrement ou déchiffrement.

Cryptographie. Vocabulaire.

- La **cryptographie** est une science qui étudie les méthodes permettant de transmettre des messages de façon confidentielle.
- **message clair** : un ensemble de données (texte, image,...) que l'on souhaite transmettre.
- Le **chiffrement** est un procédé permettant de transformer le message clair de telle sorte qu'il soit incompréhensible par qui que ce soit d'autre que l'auteur du message et le destinataire.
- Le **chiffré** est le résultat du chiffrement.
- Le **déchiffrement** est le procédé permettant de retrouver le message clair à partir du chiffré.
- La **clé** de chiffrement est un paramètre qui est utilisé dans le procédé de chiffrement ou déchiffrement.

Cryptosystème

Définition

Un **cryptosystème** est un quintuplé $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ formé de

- un ensemble de clés $\mathcal{K}$
- un ensemble de messages clairs possibles , $\mathcal{M}$,
- un ensemble de messages chiffrés possibles $\mathcal{C}$
- un algorithme de chiffrage, représenté par une fonction $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$,
- et un procédé de déchiffrage , représenté par une fonction $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$.

On suppose que pour tout $m \in \mathcal{M}$ il existe une paide de clés de chiffrement et de déchiffrement telles que la relation

$$D(k_D, E(k_E, m)) = m$$

est assurée.

Cryptosystème

Définition

Un **cryptosystème** est un quintuplé $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ formé de

- un ensemble de clés $\mathcal{K}$
- un ensemble de messages clairs possibles , $\mathcal{M}$,
- un ensemble de messages chiffrés possibles $\mathcal{C}$
- un algorithme de chiffrage, représenté par une fonction $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$,
- et un procédé de déchiffrage , représenté par une fonction $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$.

On suppose que pour tout $m \in \mathcal{M}$ il existe une paide de clés de chiffrement et de déchiffrement telles que la relation

$$D(k_D, E(k_E, m)) = m$$

est assurée.

Cryptosystème

Définition

Un **cryptosystème** est un quintuplé $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ formé de

- un ensemble de clés $\mathcal{K}$
- un ensemble de messages clairs possibles , $\mathcal{M}$,
- un ensemble de messages chiffrés possibles $\mathcal{C}$
- un algorithme de chiffrage, représenté par une fonction $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$,
- et un procédé de déchiffrage , représenté par une fonction $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$.

On suppose que pour tout $m \in \mathcal{M}$ il existe une paide de clés de chiffrement et de déchiffrement telles que la relation

$$D(k_D, E(k_E, m)) = m$$

est assurée.

Cryptosystème

Définition

Un **cryptosystème** est un quintuplé $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ formé de

- un ensemble de clés $\mathcal{K}$
- un ensemble de messages clairs possibles , $\mathcal{M}$,
- un ensemble de messages chiffrés possibles $\mathcal{C}$
- un algorithme de chiffrage, représenté par une fonction $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$,
- et un procédé de déchiffrage , représenté par une fonction $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$.

On suppose que pour tout $m \in \mathcal{M}$ il existe une paide de clés de chiffrement et de déchiffrement telles que la relation

$$D(k_D, E(k_E, m)) = m$$

est assurée.

Cryptosystème

Définition

Un **cryptosystème** est un quintuplé $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ formé de

- un ensemble de clés $\mathcal{K}$
- un ensemble de messages clairs possibles , $\mathcal{M}$,
- un ensemble de messages chiffrés possibles $\mathcal{C}$
- un algorithme de chiffrage, représenté par une fonction $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$,
- et un procédé de déchiffrage , représenté par une fonction $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$.

On suppose que pour tout $m \in \mathcal{M}$ il existe une paide de clés de chiffrement et de déchiffrement telles que la relation

$$D(k_D, E(k_E, m)) = m$$

est assurée.

Cryptosystème

Définition

Un **cryptosystème** est un quintuplé $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ formé de

- un ensemble de clés $\mathcal{K}$
- un ensemble de messages clairs possibles , $\mathcal{M}$,
- un ensemble de messages chiffrés possibles $\mathcal{C}$
- un algorithme de chiffrage, représenté par une fonction $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$,
- et un procédé de déchiffrage , représenté par une fonction $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$.

On suppose que pour tout $m \in \mathcal{M}$ il existe une paide de clés de chiffrement et de déchiffrement telles que la relation

$$D(k_D, E(k_E, m)) = m$$

est assurée.

Cryptosystème

Définition

Un **cryptosystème** est un quintuplé $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ formé de

- un ensemble de clés $\mathcal{K}$
- un ensemble de messages clairs possibles , $\mathcal{M}$,
- un ensemble de messages chiffrés possibles $\mathcal{C}$
- un algorithme de chiffrage, représenté par une fonction $E : \mathcal{K} \times \mathcal{M} \to \mathcal{C}$,
- et un procédé de déchiffrage , représenté par une fonction $D : \mathcal{K} \times \mathcal{C} \to \mathcal{M}$.

On suppose que pour tout $m \in \mathcal{M}$ il existe une paide de clés de chiffrement et de déchiffrement telles que la relation

$$D(k_D, E(k_E, m)) = m$$

est assurée.

Cryptographie. Un peu d'histoire

- Cryptographie signifie "écriture cachée" (kryptos = caché, graphein= écriture)
- Kàma-Sutra recommandait aux femmes d'apprendre 60 arts, dont les échecs, la reliure, la tapisserie et... l'écriture secrète pour cacher leur liaisons
- L'une des premières méthodes de cryptage par substitution connue est celle de César (50 av. J.C). Chaque lettre de message à transmettre était remplacée par la lettre située dans l'alphabet trois positions plus loin.
- Par exemple, *A* est remplacé par "D", "Z" par "C".

Cryptographie. Un peu d'histoire

- Cryptographie signifie "écriture cachée" (kryptos = caché, graphein= écriture)
- Kàma-Sutra recommandait aux femmes d'apprendre 60 arts, dont les échecs, la reliure, la tapisserie et... l'écriture secrète pour cacher leur liaisons
- L'une des premières méthodes de cryptage par substitution connue est celle de César (50 av. J.C). Chaque lettre de message à transmettre était remplacée par la lettre située dans l'alphabet trois positions plus loin.
- Par exemple, A est remplacé par "D", "Z" par "C".

Cryptographie. Un peu d'histoire

- Cryptographie signifie "écriture cachée" (kryptos = caché, graphein= écriture)
- Kàma-Sutra recommandait aux femmes d'apprendre 60 arts, dont les échecs, la reliure, la tapisserie et... l'écriture secrète pour cacher leur liaisons
- L'une des premières méthodes de cryptage par substitution connue est celle de César (50 av. J.C). Chaque lettre de message à transmettre était remplacée par la lettre située dans l'alphabet trois positions plus loin.
- Par exemple, A est remplacé par "D", "Z" par "C".

Cryptographie. Un peu d'histoire

- Cryptographie signifie "écriture cachée" (kryptos = caché, graphein= écriture)
- Kàma-Sutra recommandait aux femmes d'apprendre 60 arts, dont les échecs, la reliure, la tapisserie et... l'écriture secrète pour cacher leur liaisons
- L'une des premières méthodes de cryptage par substitution connue est celle de César (50 av. J.C). Chaque lettre de message à transmettre était remplacée par la lettre située dans l'alphabet trois positions plus loin.
- Par exemple, A est remplacé par "D", "Z" par "C".

Cryptographie. Un peu d'histoire.

- Les méthodes de substitution, analogues à celle de César, consistent à apparier les lettres de l'alphabet et à remplacer chaque lettre de message par la lettre de sa paire
- Elles ont été massivement utilisées jusqu'à la fin du 1er millénaire
- IXème siècle : le savant arabe AL-Kindi rédige le premier traité connu sur l'analyse fréquentielle comme technique de cryptanalyse
- Il montre comment retrouver le message en analysant les fréquences d'occurrence de caractères dans une langue donnée
- Le cryptage par substitution devient trop vulnérable

Cryptographie. Un peu d'histoire.

- Les méthodes de substitution, analogues à celle de César, consistent à apparier les lettres de l'alphabet et à remplacer chaque lettre de message par la lettre de sa paire
- Elles ont été massivement utilisées jusqu'à la fin du 1er millénaire
- IXème siècle : le savant arabe AL-Kindi rédige le premier traité connu sur l'analyse fréquentielle comme technique de cryptanalyse
- Il montre comment retrouver le message en analysant les fréquences d'occurrence de caractères dans une langue donnée
- Le cryptage par substitution devient trop vulnérable

Cryptographie. Un peu d'histoire.

- Les méthodes de substitution, analogues à celle de César, consistent à apparier les lettres de l'alphabet et à remplacer chaque lettre de message par la lettre de sa paire
- Elles ont été massivement utilisées jusqu'à la fin du 1er millénaire
- IXème siècle : le savant arabe AL-Kindi rédige le premier traité connu sur l'analyse fréquentielle comme technique de cryptanalyse
- Il montre comment retrouver le message en analysant les fréquences d'occurrence de caractères dans une langue donnée
- Le cryptage par substitution devient trop vulnérable

Cryptographie. Un peu d'histoire.

- Les méthodes de substitution, analogues à celle de César, consistent à apparier les lettres de l'alphabet et à remplacer chaque lettre de message par la lettre de sa paire
- Elles ont été massivement utilisées jusqu'à la fin du 1er millénaire
- IXème siècle : le savant arabe AL-Kindi rédige le premier traité connu sur l'analyse fréquentielle comme technique de cryptanalyse
- Il montre comment retrouver le message en analysant les fréquences d'occurrence de caractères dans une langue donnée
- Le cryptage par substitution devient trop vulnérable

Cryptographie. Un peu d'histoire.

- Les méthodes de substitution, analogues à celle de César, consistent à apparier les lettres de l'alphabet et à remplacer chaque lettre de message par la lettre de sa paire
- Elles ont été massivement utilisées jusqu'à la fin du 1er millénaire
- IXème siècle : le savant arabe AL-Kindi rédige le premier traité connu sur l'analyse fréquentielle comme technique de cryptanalyse
- Il montre comment retrouver le message en analysant les fréquences d'occurrence de caractères dans une langue donnée
- Le cryptage par substitution devient trop vulnérable

Cryptographie. Notion de sécurité.

Principe de A. Kerckhoffs (fin XIXe)

La sécurité d'un cryptosystème ne doit pas reposer sur la non divulgation de la fonction de cryptage mais uniquement sur la non divulgation de la clé.

Sécurité : approche de Shannon

- 1949. Publication par C. Shannon de l'article "Communication Theory of Secrecy Systems" dans la revue Bell System Technical Journal.
- Le concept d'entropie est utilisé pour analyser et quantifier la sécurité d'un cryptosystème.

Sécurité : approche de Shannon

- 1949. Publication par C. Shannon de l'article "Communication Theory of Secrecy Systems" dans la revue Bell System Technical Journal.
- Le concept d'entropie est utilisé pour analyser et quantifier la sécurité d'un cryptosystème.

Cryptosystème parfaitement sûr

- On associe aux cryptosystème $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ trois variables aléatoires :
- $M \in \mathcal{M}$ représente le choix d'un message clair
- $K \in \mathcal{K}$ représente le choix d'une clé
- $C \in \mathcal{C}$ représente le choix d'un chiffré
- on suppose que le message clair et la clé sont choisis de façon indépendante

Cryptosystème parfaitement sûr

- On associe aux cryptosystème $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ trois variables aléatoires :
- $M \in \mathcal{M}$ représente le choix d'un message clair
- $K \in \mathcal{K}$ représente le choix d'une clé
- $C \in \mathcal{C}$ représente le choix d'un chiffré
- on suppose que le message clair et la clé sont choisis de façon indépendante

Cryptosystème parfaitement sûr

- On associe aux cryptosystème $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ trois variables aléatoires :
- $M \in \mathcal{M}$ représente le choix d'un message clair
- $K \in \mathcal{K}$ représente le choix d'une clé
- $C \in \mathcal{C}$ représente le choix d'un chiffré
- on suppose que le message clair et la clé sont choisis de façon indépendante

Cryptosystème parfaitement sûr

- On associe aux cryptosystème $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ trois variables aléatoires :
- $M \in \mathcal{M}$ représente le choix d'un message clair
- $K \in \mathcal{K}$ représente le choix d'une clé
- $C \in \mathcal{C}$ représente le choix d'un chiffré
- on suppose que le message clair et la clé sont choisis de façon indépendante

Cryptosystème parfaitement sûr

- On associe aux cryptosystème $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$ trois variables aléatoires :
- $M \in \mathcal{M}$ représente le choix d'un message clair
- $K \in \mathcal{K}$ représente le choix d'une clé
- $C \in \mathcal{C}$ représente le choix d'un chiffré
- on suppose que le message clair et la clé sont choisis de façon indépendante

Cryptosystème parfaitement sûr

Définition

Soit un cryptosystème $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$. Soient M et C les variables aléatoires représentant le choix d'un message claire et d'un chiffré. Le système est dit parfaitement sûr ssi

$$H(M|C) = H(M)$$

La connaissance du chiffré n'apporte aucune information sur le message clair.

Cryptosystème parfaitement sûr

Définition

Soit un cryptosystème $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$. Soient M et C les variables aléatoires représentant le choix d'un message claire et d'un chiffré. Le système est dit parfaitement sûr ssi

$$H(M|C) = H(M)$$

La connaissance du chiffré n'apporte aucune information sur le message clair.

Exemple de chiffrement parfaitement sûr : le chiffre de Vernam

- Cette méthode a été proposée en 1917.
- Les messages clairs sont des suites de bits de longueur n. L'espace des messages est alors $\mathcal{M} = 0,1^n$.
- Les clés sont les suites binaires de même longueur que les messages : $\mathcal{K} = \mathcal{M} = 0,1^n$.
- La fonction de chiffrement : pour tout $m = m_1 \dots m_n$ et pour tout $k = k_1 \dots k_n$

$$c = E(k, m) = k \oplus m = m_1 \oplus k_1 \dots m_n \oplus k_n$$

Exemple de chiffrement parfaitement sûr : le chiffre de Vernam

- Cette méthode a été proposée en 1917.
- Les messages clairs sont des suites de bits de longueur n. L'espace des messages est alors $\mathcal{M} = 0,1^n$.
- Les clés sont les suites binaires de même longueur que les messages : $\mathcal{K} = \mathcal{M} = 0,1^n$.
- La fonction de chiffrement : pour tout $m = m_1 \dots m_n$ et pour tout $k = k_1 \dots k_n$

$$c = E(k, m) = k \oplus m = m_1 \oplus k_1 \dots m_n \oplus k_n$$

Exemple de chiffrement parfaitement sûr : le chiffre de Vernam

- Cette méthode a été proposée en 1917.
- Les messages clairs sont des suites de bits de longueur n. L'espace des messages est alors $\mathcal{M} = 0,1^n$.
- Les clés sont les suites binaires de même longueur que les messages : $\mathcal{K} = \mathcal{M} = 0,1^n$.
- La fonction de chiffrement : pour tout $m = m_1 \dots m_n$ et pour tout $k = k_1 \dots k_n$

$$c = E(k, m) = k \oplus m = m_1 \oplus k_1 \dots m_n \oplus k_n$$

Exemple de chiffrement parfaitement sûr : le chiffre de Vernam

- Cette méthode a été proposée en 1917.
- Les messages clairs sont des suites de bits de longueur n. L'espace des messages est alors $\mathcal{M} = 0, 1^n$.
- Les clés sont les suites binaires de même longueur que les messages : $\mathcal{K} = \mathcal{M} = 0, 1^n$.
- La fonction de chiffrement : pour tout $m = m_1 \dots m_n$ et pour tout $k = k_1 \dots k_n$

$$c = E(k, m) = k \oplus m = m_1 \oplus k_1 \dots m_n \oplus k_n$$

Exemple de chiffrement parfaitement sûr : le chiffre de Vernam

Proposition

Le chiffrement de Vernam est parfaitement sur

Théorème

Dans un système cryptographique parfaitement sûr on a

$$H(K) \geq H(M)$$

En particulier, si tous les messages et toutes les clés sont équiprobables, les clés sont de longueur au moins égale à celle des messages.

Exemple de chiffrement parfaitement sûr : le chiffre de Vernam

Proposition

Le chiffrement de Vernam est parfaitement sur

Théorème

Dans un système cryptographique parfaitement sûr on a

$$H(K) \geq H(M)$$

En particulier, si tous les messages et toutes les clés sont équiprobables, les clés sont de longueur au moins égale à celle des messages.

Attention ! Un chiffrement parfaitement sûr n'est pas invulnérable !

- Dans le cas de chiffrement de Vernam il suffit d'un bloc de message clair pour découvrir la clé :

$$k = c \oplus m$$

- Il est alors nécessaire de changer de clé à chaque bloc ; d'où le nom de "masque jetable" ;
- En pratique, cette procédure et très lourde : les clés ont la même longueur que les messages
- Ce chiffrement a été utilisé pour le téléphone rouge : la clé a été envoyé par porteur

Attention ! Un chiffrement parfaitement sûr n'est pas invulnérable !

- Dans le cas de chiffrement de Vernam il suffit d'un bloc de message clair pour découvrir la clé :

$$k = c \oplus m$$

- Il est alors nécessaire de changer de clé à chaque bloc ; d'où le nom de "masque jetable" ;
- En pratique, cette procédure et très lourde : les clés ont la même longueur que les messages
- Ce chiffrement a été utilisé pour le téléphone rouge : la clé a été envoyé par porteur

Attention ! Un chiffrement parfaitement sûr n'est pas invulnérable !

- Dans le cas de chiffrement de Vernam il suffit d'un bloc de message clair pour découvrir la clé :

$$k = c \oplus m$$

- Il est alors nécessaire de changer de clé à chaque bloc ; d'où le nom de "masque jetable" ;
- En pratique, cette procédure et très lourde : les clés ont la même longueur que les messages
- Ce chiffrement a été utilisé pour le téléphone rouge : la clé a été envoyé par porteur

Attention ! Un chiffrement parfaitement sûr n'est pas invulnérable !

- Dans le cas de chiffrement de Vernam il suffit d'un bloc de message clair pour découvrir la clé :

$$k = c \oplus m$$

- Il est alors nécessaire de changer de clé à chaque bloc ; d'où le nom de "masque jetable" ;
- En pratique, cette procédure et très lourde : les clés ont la même longueur que les messages
- Ce chiffrement a été utilisé pour le téléphone rouge : la clé a été envoyé par porteur

Et si les clés sont plus courtes ? Quelques définitions.

- Soit un langage composé de mots de longueur donnée N sur un alphabet donné A. On associe la variable aléatoire M au choix au hasard d'un mot du langage.
- Taux du langage (ou taux d'entropie)

$$r = \lim_{N \to \infty} \frac{H(M)}{N}$$

représente la quantité moyenne d'information par caractère de message
- Si le nombre de caractères de l'alphabet est L on appelle taux maximal du langage la quantité

$$R = log_2 L$$

Il s'agit de l'entropie maximale d'un caractère
- Enfin on appelle redondance du langage la différence

$$D = R - r$$

Et si les clés sont plus courtes ? Quelques définitions.

- Soit un langage composé de mots de longueur donnée N sur un alphabet donné A. On associe la variable aléatoire M au choix au hasard d'un mot du langage.
- Taux du langage (ou taux d'entropie)

$$r = \lim_{N \to \infty} \frac{H(M)}{N}$$

représente la quantité moyenne d'information par caractère de message

- Si le nombre de caractères de l'alphabet est L on appelle taux maximal du langage la quantité

$$R = log_2 L$$

Il s'agit de l'entropie maximale d'un caractère

- Enfin on appelle redondance du langage la différence

$$D = R - r$$

Et si les clés sont plus courtes ? Quelques définitions.

- Soit un langage composé de mots de longueur donnée N sur un alphabet donné A. On associe la variable aléatoire M au choix au hasard d'un mot du langage.
- Taux du langage (ou taux d'entropie)

$$r = \lim_{N \to \infty} \frac{H(M)}{N}$$

  représente la quantité moyenne d'information par caractère de message
- Si le nombre de caractères de l'alphabet est L on appelle taux maximal du langage la quantité

$$R = log_2 L$$

  Il s'agit de l'entropie maximale d'un caractère
- Enfin on appelle redondance du langage la différence

$$D = R - r$$

Et si les clés sont plus courtes ? Quelques définitions.

- Soit un langage composé de mots de longueur donnée N sur un alphabet donné A. On associe la variable aléatoire M au choix au hasard d'un mot du langage.
- Taux du langage (ou taux d'entropie)

$$r = \lim_{N \to \infty} \frac{H(M)}{N}$$

  représente la quantité moyenne d'information par caractère de message
- Si le nombre de caractères de l'alphabet est L on appelle taux maximal du langage la quantité

$$R = log_2 L$$

  Il s'agit de l'entropie maximale d'un caractère
- Enfin on appelle redondance du langage la différence

$$D = R - r$$

Distance d'unicité

Définition

Soit un cryptosystème $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$. On appelle la distance d'unicité le plus petit nombre de messages chiffrés dont il est nécessaire disposer pour que l'incertitude résiduelle sur la clé sachant ces chiffrés soit nulle :

$$n_0 : \ H(K|C_1, \ldots, C_{n_0}) = 0$$

Attention

Il faut interpréter cette définitoion dans le sens suivant : si l'on ne dispose pas de longueur suffisante de message chiffré donnée par la distance d'unicité, il est impossible de déterminer la clé avec certitude.
Ce résultat ne permet surtout pas de se prononcer sur la puissance de calcul nécessaire pour découvrir la clé ni sur les moyens d'y parvenir.

Distance d'unicité

Définition

Soit un cryptosystème $(\mathcal{K}, \mathcal{M}, \mathcal{C}, E, D)$. On appelle la distance d'unicité le plus petit nombre de messages chiffrés dont il est nécessaire disposer pour que l'incertitude résiduelle sur la clé sachant ces chiffrés soit nulle :

$$n_0 : \ H(K|C_1, \ldots, C_{n_0}) = 0$$

Attention

Il faut interpréter cette définitoion dans le sens suivant : si l'on ne dispose pas de longueur suffisante de message chiffré donnée par la distance d'unicité, il est impossible de déterminer la clé avec certitude.
Ce résultat ne permet surtout pas de se prononcer sur la puissance de calcul nécessaire pour découvrir la clé ni sur les moyens d'y parvenir.

Distance d'unicité

Proposition

La distance d'unicité d d'un cryptosystème est égale à

$$d = \frac{H(K)}{D} = \frac{H(K)}{R - r}$$

où D est la redondance du langage.

Attention

La distance d'unicité est inversement proportionnelle à la redondance des messages clairs.
Pour améliorer la distance d'unicité, il est préférable de traiter en amont les messages de façon à réduire la redondance. Par exemple, une compression sans pertes par codage de Huffman ou autre peut être utilisée avant le chiffrement.

Distance d'unicité

Proposition

La distance d'unicité d d'un cryptosystème est égale à

$$d = \frac{H(K)}{D} = \frac{H(K)}{R - r}$$

où D est la redondance du langage.

Attention

La distance d'unicité est inversement proportionnelle à la redondance des messages clairs.
Pour améliorer la distance d'unicité, il est préférable de traiter en amont les messages de façon à réduire la redondance. Par exemple, une compression sans pertes par codage de Huffman ou autre peut être utilisée avant le chiffrement.

Distance d'unicité : exemple

- Considérons un chiffrement par substitution.
- La clé est alors une permutation quelconque de l'alphabet latin σ.
- Chaque lettre m_i d'un message $m = m_1, \ldots, m_n$ est remplacée par $\sigma(m_i)$
- L'ensemble des clés est alors l'ensemble de toutes les permutations possibles
- $H(K) = \log_2(26!)$
- Pour le français on a $r \simeq 3.97$, $R = 4.67$. Ainsi la redondance est $D = 0.7$.
- on obtient alors la distance d'unicité d'un chiffrement par substitution :

$$d = \frac{H(K)}{D} = \frac{log_2(26!)}{0.7} \simeq 126$$

Distance d'unicité : exemple

- Considérons un chiffrement par substitution.
- La clé est alors une permutation quelconque de l'alphabet latin σ.
- Chaque lettre m_i d'un message $m = m_1, \ldots, m_n$ est remplacée par $\sigma(m_i)$
- L'ensemble des clés est alors l'ensemble de toutes les permutations possibles
- $H(K) = \log_2(26!)$
- Pour le français on a $r \simeq 3.97$, $R = 4.67$. Ainsi la redondance est $D = 0.7$.
- on obtient alors la distance d'unicité d'un chiffrement par substitution :

$$d = \frac{H(K)}{D} = \frac{log_2(26!)}{0.7} \simeq 126$$

Distance d'unicité : exemple

- Considérons un chiffrement par substitution.
- La clé est alors une permutation quelconque de l'alphabet latin σ.
- Chaque lettre m_i d'un message $m = m_1, \ldots, m_n$ est remplacée par $\sigma(m_i)$
- L'ensemble des clés est alors l'ensemble de toutes les permutations possibles
- $H(K) = \log_2(26!)$
- Pour le français on a $r \simeq 3.97$, $R = 4.67$. Ainsi la redondance est $D = 0.7$.
- on obtient alors la distance d'unicité d'un chiffrement par substitution :

$$d = \frac{H(K)}{D} = \frac{log_2(26!)}{0.7} \simeq 126$$

Distance d'unicité : exemple

- Considérons un chiffrement par substitution.
- La clé est alors une permutation quelconque de l'alphabet latin σ.
- Chaque lettre m_i d'un message $m = m_1, \ldots, m_n$ est remplacée par $\sigma(m_i)$
- L'ensemble des clés est alors l'ensemble de toutes les permutations possibles
- $H(K) = \log_2(26!)$
- Pour le français on a $r \simeq 3.97$, $R = 4.67$. Ainsi la redondance est $D = 0.7$.
- on obtient alors la distance d'unicité d'un chiffrement par substitution :

$$d = \frac{H(K)}{D} = \frac{log_2(26!)}{0.7} \simeq 126$$

Distance d'unicité : exemple

- Considérons un chiffrement par substitution.
- La clé est alors une permutation quelconque de l'alphabet latin σ.
- Chaque lettre m_i d'un message $m = m_1, \ldots, m_n$ est remplacée par $\sigma(m_i)$
- L'ensemble des clés est alors l'ensemble de toutes les permutations possibles
- $H(K) = \log_2(26!)$
- Pour le français on a $r \simeq 3.97$, $R = 4.67$. Ainsi la redondance est $D = 0.7$.
- on obtient alors la distance d'unicité d'un chiffrement par substitution :

$$d = \frac{H(K)}{D} = \frac{log_2(26!)}{0.7} \simeq 126$$

Distance d'unicité : exemple

- Considérons un chiffrement par substitution.
- La clé est alors une permutation quelconque de l'alphabet latin σ.
- Chaque lettre m_i d'un message $m = m_1, \ldots, m_n$ est remplacée par $\sigma(m_i)$
- L'ensemble des clés est alors l'ensemble de toutes les permutations possibles
- $H(K) = \log_2(26!)$
- Pour le français on a $r \simeq 3.97$, $R = 4.67$. Ainsi la redondance est $D = 0.7$.
- on obtient alors la distance d'unicité d'un chiffrement par substitution :

$$d = \frac{H(K)}{D} = \frac{log_2(26!)}{0.7} \simeq 126$$

Distance d'unicité : exemple

- Considérons un chiffrement par substitution.
- La clé est alors une permutation quelconque de l'alphabet latin σ.
- Chaque lettre m_i d'un message $m = m_1, \ldots, m_n$ est remplacée par $\sigma(m_i)$
- L'ensemble des clés est alors l'ensemble de toutes les permutations possibles
- $H(K) = \log_2(26!)$
- Pour le français on a $r \simeq 3.97$, $R = 4.67$. Ainsi la redondance est $D = 0.7$.
- on obtient alors la distance d'unicité d'un chiffrement par substitution :

$$d = \frac{H(K)}{D} = \frac{log_2(26!)}{0.7} \simeq 126$$