Séance 3 - Travaux Dirigés
Entropie, Information et Chiffrements parfaits

Yann Rotella

2026

L'objectif de cette séance est de se familiariser avec les notions d'information et d'entropie (cours 2), en lien avec la cryptographie. Cette séance est entièrement seule et il n'y a pas de travail en groupe.

Indication : la fonction $\log_2$ vérifie $\log_2 z < (z-1)\log_2(e)$ si $z > 0, z \neq 1$ et égalité sinon.

Exercice 1. *Le théorème de Shannon.*
On va montrer le théorème vu en cours.

(1) Rappeler la définition de chiffrement inconditionnellement sûr
(2) Se rappeler pourquoi, quand deux v.a. ne sont pas indépendantes, $I(X;Y) > 0$
(3) Noter les hypothèses du théorème de Shannon.
(4) Enoncer le théorème de Shannon.
(5) Soient $m \in \mathcal{M}$ et $c \in \mathcal{C}$. En utilisant la loi des probabilités totales sur les clefs, exprimer $p(m,c)$ et $p(c)$. Donner ensuite la relation entre $p(m|c)$ et $p(c|m)$.
(6) Ecrire la formule de $H(M|C)$.
(7) Montrer le théorème de Shannon (on commencera par le sens indirect puis les sens direct).
(8) Montrer que si l'espace des messages est plus grand que l'espace des clefs, alors aucun système n'admet une sécurité parfaite.

Exercice 2. *Entropie et Information de la clef, du message et du chiffré.*
L'objectif de cet exercice est de quantifier, en fonction de la taille du message, de la taille de la clef et de certaines hypothèses quand est-ce qu'on peut, théoriquement, retrouver la clef secrète.

(1) Rappeler les différents modèles d'attaque vus en cours et décrivez-les.
(2) Rappeler le chiffrement de Vernam.
(3) Expliquer pourquoi, même dans un modèle à clairs choisis (le plus fort), le chiffrement de Vernam reste sécurisé.
(4) Soient X et Y deux v.a., montrer que

$$H(X|Y) \leq H(X)$$

avec égalité si et seulement si les v.a. sont indépendantes.
(5) Montrer que, pour toute v.a. X et Y, on a

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

(6) Montrer que $\log_2(\#\mathcal{X}) \geq H(X) \geq 0$.

On considère maintenant un chiffrement E, et les trois v.a. associées K, M et C décrivant respectivement la clef secrète, le message et le texte chiffré.

(7) Est-ce réaliste de considérer que K et M sont indépendantes ?

(8) Que valent $H(C|M,K)$ et $H(M|C,K)$?

(9) En utilisant la question 5, montrer que

$$H(C,M,K) = H(C|M,K) + H(M|K) + H(K)$$

(10) Écrire de la même manière $H(K,C,M)$

(11) En déduire que

$$H(K|M,C) \geq H(K) - H(C)$$

On suppose maintenant que C et M sont indépendantes.

(12) Est-ce que cette hypothèse est réaliste ?

(13) Est-ce que si ce n'est pas le cas c'est un problème ?

On suppose maintenant M et C suivent une loi uniforme sur $\{0,1\}^n$ et que les clefs sont tirées uniformément dans $\{0,1\}^\kappa$

(14) Que vaut $H(M)$ et $H(C)$?

(15) Que vaut $H(K)$?

(16) Avec toutes ces hypothèses, que vaut $H(K|M,C)$? Quelle est l'interprétation de cette valeur ?

(17) D'après la question 6, l'entropie est toujours positive. Que se passe t'il quand $n > \kappa$?

Exercices complémentaires

Exercice 3. *Ordres de grandeur.*
Dans cet exercice, on ne cherchera pas à calculer la valeur exacte, mais des approximations, à chaque fois en puissance de 2 ou en puissances de 10.
Indication : $2^{10} = 1024 \approx 10^3$.

(1) Combien y'a t'il de secondes dans une année ?

(2) On suppose maintenant que l'on a accès à un PC (Intel Core i7 5960x) qui peut effectuer 300000 millions d'instructions par seconde (MIPs). Combien d'instructions peut réaliser notre ordinateur en une année ?

(3) On suppose maintenant que l'algorithme de chiffrement nécessite 100 instructions, que le chiffrement utilise une clef de taille 64 bits et que l'attaquant possède un couple clair-chiffré. Combien de temps prendrait l'attaque par recherche exhaustive avec un seul PC ?

(4) Calculer le temps de l'attaque avec 100, 1000 et 100 000 ordinateurs de ce type et pour des clefs de taille 56, 64 et 128 bits.

(5) Même question avec un supercalculateur (rechercher le nombre de FLOPS des supercalculateurs actuels).

Exercice 4. *Exemple de chiffrement inconditionnellement sûr.*
On souhaite transmettre des résultats de lancers de deux dés de manière sécurisée.

(1) Donner la taille de l'espace des messages clairs.

(2) Donner la distribution de probabilités des messages transmis.

(3) Rappeler la formule de l'entropie. À quoi l'entropie correspond-t-elle ? (plusieurs réponses peuvent fonctionner)

(4) Calculer $H(M)$ où M est une v.a. correspondant aux clairs (on pourra utiliser un ordinateur).

(5) Donner la taille minimale d'espace des clefs pour avoir un chiffrement inconditionnellement sûr.

(6) Décrire entièrement un chiffrement inconditionnellement sûr qui chiffrerait respectivement les résultats d'un, deux et trois lancers de dés.

Exercice 5. *Entropie et mots de passe.*
On regarde l'ensemble des mots de passe possibles. En pratique, certains mots de passe sont plus utilisés que d'autre. On regarde donc $\mathcal{M}$ l'ensemble des mots de passe possibles et on regarde la distribution de probabilités de ceux-ci. On peut montrer (mais c'est hors programme) que le temps moyen pour trouver un mot de passe en les testant tous dans l'ordre décroissant des probabilités est de $2^{H(M)}$ où $H(M)$ est l'entropie des mots de passe.

(1) Calculer $H(M)$ quand $\#\mathcal{M} = 10^6$ et que la dsitribution est uniforme.

(2) Calculer $H(M)$ quand 70% des mots de passe sont pris uniformément dans $\mathcal{S}_{frequent}$ de taille 10^6 et 30% de manière uniforme dans un ensemble de taille N arbitraire.

(3) Donner une valeur de N suffisante pour que l'entropie soit assez grande.

(4) Est-ce que c'est effectivement suffisant en pratique au niveau de la sécurité ?